Міністерство освіти і науки України

Національний університет «Києво-Могилянська академія»

Факультет правничих наук
Кафедра приватного права

Магістерська робота

Освітній ступінь - магістр

на тему: «**СТАНДАРТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ**»

«The standards of the data protection in the European Union»

Виконав студент 2-го року навчання

Спеціальності

081 Правознавство

Дейнека Євгеній Віталійович

Керівник магістерської роботи:

Смирнова Тетяна Сергіївна

кандидат юридичних наук, доцент

Рецензент _____

Магістерська робота захищена

З оцінкою _____

Секретар ЕК _____

«__» _____ 20____ р.

Київ 2021

Декларація

академічної доброчесності

студента/ студентки НаУКМА

Я Дейнека Євгеній Віталійович,
студент(ка) II року навчання факультету правничих наук,
спеціальність Правознавство 081,
адреса електронної пошти zheniadeineka98@gmail.com

- підтверджую, що написана мною кваліфікаційна/магістерська робота на тему «Стандарти захисту персональних даних в Європейському Союзі» відповідає вимогам академічної доброчесності та не містить порушень, передбачених пунктами 3.1.1-3.1.6 Положення про академічну доброчесність здобувачів НаУКМА від 07.03.2018 року, зі змістом якого ознайомлений/ ознайомлена;
- підтверджую, що надана мною електронна версія роботи є остаточною і готовою до перевірки;
- згоден/ згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності, у будь-який спосіб, у тому числі порівняння змісту роботи та формування звіту подібності за допомогою електронної системи Unicheck.
- даю згоду на архівування моєї роботи в репозитаріях та базах даних університету для порівняння цієї та майбутніх робіт.

12.05.2021		Дейнека Є.В.
Дата	*Підпис*	*Прізвище, ініціали*

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

GDPR	General data protection regulation
ICO	Британський наглядовий орган у сфері захисту персональних даних
EDPB	European Data Protection Board
DPO	Data protection officer
EDPS	European Data Protection Supervisor
DPA	Data protection act, основний закон, що регулює сферу захисту персональних даних у Великій Британії
PERC	Privacy and Electronic Communications Regulations, закон спрямований на регулювання обігу персональних даних у цифровій сфері
AEPD	Agencia Espanila Protetion Datos, іспанський наглядовий орган у сфері захисту персональних даних
PDPC	Personal Data Protection Code, основний закон, що регулює сферу захисту персональних даних у Італії
IDPA	Garante per la protezione dei dati personali, італійський наглядовий орган у сфері захисту персональних даних
NAIH	Nemzeti Ada tvedelmi es Informacioszabadsag Hatosag, угорський наглядовий орган у сфері захисту персональних даних
BDGS	Bundesdatenschutzgesetz, німецький закон про захист персональних даних
BDI	Der Bundesbeauftragte fur Datenschutz und die informationsfreiheit, німецький наглядовий орган у сфері захисту персональних даних

ВСТУП

Актуальність тематики дослідження. Сучасний бурхливий розвиток інформаційних технологій у всьому світі став яскравим свідченням переходу людського суспільства на новий, постіндустріальний рівень розвитку. За останні десятиліття людина «передоручила» пристроям величезну частину роботи, яку до цього виконувала власноруч.

Що найголовніше, цей розвиток гармонійно продовжується й надалі, і сьогодні ми не маємо однозначних підстав говорити про те, що він припиниться у найближчому майбутньому. Паралельно з цим розвитком інформаційних технологій, виникають як нові виклик, так і нові ризики для правових систем різних країн.

Не винятковою є і сфера захисту персональних даних. Попри відносно нещодавній початок свого розвитку, захист персональних даних прогресивно набуває актуальності та вагомості для кожної людини. Особливо яскраво це можна побачити в контексті застосування у цій сфері сучасних технологій, механізми роботи яких не завжди зрозумілі для кожної особи.

З огляду на це, правове регулювання сфери захисту персональних даних набуло одного з пріоритетних значень та стало каталізатором розвитку суспільства. Одним із лідерів у запровадженні такого регулювання можна назвати Європейський Союз, чий General Data Protection Regulation є одним з найбільш прогресивних документів у сфері захисту персональних даних. На додачу до цього, окремі положення GDPR про екстериторіальність його дії, свідчать про намагання ЄС встановити і «нав'язати» високі стандарти захисту персональних даних іншим країнам. Водночас для України ця тематика стає актуальною не лише в контексті екстериторіальності дії GDPR, але й через проєвропейські прагнення нашої держави.

В той же час, GDPR містить велику кількість нових концепцій та нових інститутів, які в корені змінюють вимоги щодо захисту персональних даних і які неоднозначно сприймалися щодо можливості їх практичного застосування. Такі

перестороги стосувалися не тільки контролерів та операторів персональних даних, але і держав-членів ЄС та наглядові органи. Проте, оскільки з моменту набрання чинності GDPR пройшло вже досить багато часу, можна стверджувати, що держави-члени ЄС вибудували захист персональних даних у своїх країнах відповідно до GDPR і наглядові органи цих країн мають достатні об'єми напрацьованої практики розгляду окремих порушень GDPR, на основі яких можна робити висновки щодо правозастосовності таких положень.

З огляду на це, **метою** мого **дослідження** буде аналіз положень GDPR, з урахуванням специфіки його дії в окремих державах-членах ЄС, при їх правозастосуванні та їх відповідності викликам сучасного суспільства.

Для досягнення поставленої мети необхідним є виконання наступних завдань:

- Вивчення теоретичних аспектів основних положень GDPR, які впливають на діяльність всіх суб'єктів сфери захисту персональних даних (принципи обробки даних, територіальна дія GDPR, відповідальність за GDPR та повноваження наглядових органів окремих країн);
- Огляд особливостей законодавства у сфері захисту персональних даних різних держав-членів ЄС;
- Аналіз специфіки формування та діяльності наглядових органів цих держав-членів;
- Дослідження практики розгляду спорів пов'язаних з GDPR у цих державах та аналіз кейсів з інших країн;
- Вивчення можливості взаємодії та впливу GDPR з викликами та сучасними проблемами сфери захисту персональних даних;
- Порівняння правового регулювання сфери захисту персональних даних за GDPR та в рамках Ради Європи.

З огляду на це, **об'єктом** мого **дослідження** будуть правовідносини, що виникають у сфері захисту персональних даних в різних державах-членах ЄС. Водночас **предметом** мого **дослідження** будуть норми GDPR та інших

нормативно-правових актів у сфері захисту персональних даних, які діють у Європі та практика їх правозастосування.

Методика мого **дослідження** буде поєднувати, як загальнонаукові та спеціально-наукові методи дослідження і включатиме аналітичний та синтетичний методи, статистичний, інституційний та системний, порівняльно-правовий, формально-юридичний та функціональний метод.

Магістерська робота складається із вступу, двох розділів та висновків та списку використаних джерел, загальним обсяг 109 сторінок, з яких основного тексту 88 сторінок.

РОЗДІЛ 1. Механізм захисту персональних даних за законодавством ЄС

1.1 Загальна характеристика GDRP як основного акту ЄС в сфері захисту персональних даних

З набуттям чинності GDPR у 2018 році, механізм захисту персональних даних в Європейському Союзі зазнав багатьох змін. В межах свого аналізу, я маю на меті здійснити огляд теоретичних положень GDPR, які найчастіше застосовуються контролюючими органами країн ЄС при розгляді справ, що стосуються персональних даних.

1.1.1 Основоположні принципи обробки персональних даних

Для GDPR, як для регламенту Європейського Союзу, який повинен поєднати в собі і враховувати особливості різних правових систем Європи, належне обґрунтування та визначення принципів, на яких він побудований, є надзвичайно важливим. Крім того, принципи, які закріплено в статті 5 GDPR, є основою захисту персональних даних, оскільки саме вони повинні формувати основні тенденції та підходи до сфери захисту персональних даних.

На вебсайті ICO, наглядового органу у сфері захисту персональних даних Сполученого королівства, зазначено, що: «Дотримання духу цих ключових принципів є фундаментальним елементом у побудові належної практики захисту персональних даних. Також це є ключовим елементом для дотримання всього GDPR» [1] *(тут і далі, якщо не зазначено інше – переклад мій власний (прим. – Дейнека Є.)*.

Перший та основоположний, на мій погляд, принцип, з врахуванням якого розкриваються всі інші принципи, це – «lawfulness, fairness and transparency» [2]. В українському перекладі GDPR цей принцип перекладено, як «законність, правомірність і прозорість» [3].

Сутність цього принципу, за словами Даниїла Шарова, полягає у тому, що: «Особа, яка здійснює збір персональних даних, повинна мати чітке пояснення того, з якою метою вона збирає ці дані та яким чином дані будуть нею використовуватися». [4]

Дещо по-іншому цей принцип розкривається у checklist ICO, де увага надається чотирьом основним аспектам, які мають бути дотримані щодо цього принципу, зокрема:

- «Повинна бути ідентифікована належна підстава для збору персональних даних;
- Повинна бути певність особи, що збирає персональні дані у тому, що вона при цьому не порушує жодні інші закони;
- Повинна бути впевненість у тому, що використання персональних даних здійснюється справедливим шляхом. Тобто дані повинні обробляти у такий спосіб, щоб така обробка не була пагубна, несподівана чи оманлива для осіб;
- Особи, що збирають дані мають бути від початку чіткими, відкритими та чесними щодо шляхів використання персональних даних».[5]

Таким чином зрозуміло, що цей принцип вміщує в собі необхідність дотримання інших законів, розуміння цілей використання даних, готовність комунікувати з особою, чиї персональні дані обробляються. Відповідно, цей принцип охоплює всі сфери та етапи захисту персональних даних.

Наступним принципом є принцип “purpose limitation”. Джеральдін Строубрідж щодо цього принципу пише про те, що: «Персональні дані повинні використовуватися лише з визначеною метою і повинні використовуватися для будь-яких інших цілей щодо яких особа, чиї дані збираються не надавала згоди» [6]. Варто зауважити, що GDPR не встановлено чітких критеріїв, завдяки яким можна визначити дотримання чи недотримання мети використання даних. Наглядовий орган Ірландії у своєму чек-листі пише про те, що обробка даних «буде вважатися сумісною з початковою метою залежно від будь-якого зв’язку з цією метою, контексту в якому були зібрані персональні дані, природи таких

даних, потенційних наслідків обробки для індивідів та наявності запобіжних заходів» [7].

Водночас GDPR містить ряд винятків, які дозволяють використовувати дані без порушення вказаного принципу. Так стаття 5 GDPR передбачає, що «подальше опрацювання для досягнення цілей суспільних інтересів … цілей наукового чи історичного дослідження або статистичних цілей не можна вважати… несумісним з первинними цілями» [3]. Тобто навіть, якщо особа погоджується на обробку даних з зовсім іншої метою, вона повинна розуміти, що суб'єкт, якому надаються дані, може також використовувати їх в указаних вище цілях.

В той же час, ірландський наглядовий орган наголошує на тому, що: «мета цього принципу у тому, щоб контролери будуть зрозумілими та відкритими від самого початку обробки даних щодо цілей і щоб ці цілі відповідали розумним очікуванням індивідів» [7]

Третім принципом за GDPR є «мінімізація даних»[3]. За словами Punit Bhatia, цей принцип полягає у тому, що: «під час збору даних можуть вимагатись лише персональні дані, абсолютно необхідні для цієї мети» [8].

Окремі аспекти цього принципу також розкриває ICO. Зокрема, Checklist британського органу містить не лише пояснення щодо найменшої кількості даних, але і щодо достатності даних для виконання поставлених цілей і про необхідність регулярного аналізу даних та видалення тих, що вже не є необхідними [9]. На цьому прикладі, ми бачимо, що суб'єкти, які здійснюють обробку даних, повинні регулярно їх перевіряти, що вже тягне зобов'язання для цих суб'єктів мати обґрунтоване пояснення щодо всіх даних, що наявні у такого суб'єкта в будь-який момент часу.

Крім того, останній пункт, в свою чергу, перекликається відразу з кількома наступними принципами. Зокрема про необхідність оновлення даних так само передбачена принципом "accuracy". Згідно з цим принципом, необхідно, щоб дані були точними, оновлювалися та могли виправлятися особою, чиї дані збираються. [3]

Для дотримання цього принципу «контролер повинен забезпечити наявність у нього систем для внесення змін або видалення неточних або застарілих персональних даних» [10]. Як і щодо інших принципів, GDPR не встановлює ніяких вимог щодо того, яким саме чином повинно бути організовано виконання контролерами цього принципу. Водночас зрозуміло, що суб'єкти можуть у будь-який момент звертатися з тим, щоб їх дані були виправленні чи видалені і більше не опрацьовувалися. В той же час, цей принцип є зобов'язальним лише для контролерів даних і не створює зобов'язання для суб'єктів даних.

Наступним принципом GDPR, який так само перекликається, на мою думку, з «data minimization», е принцип «storage limitation». Цей принцип встановлює часові обмеження щодо можливості обробки персональних даних. Галина Кулакова пише про те, що згідно з цим принципом «суб'єктам доведеться встановити певний строк для зберігання персональних даних та обгрунтувати необхідність такого періоду, з огляду на конкретні цілі»[11]. Однак GDRP не встановлює зобов'язання мати безпосередньо чіткий строк, у календарних днях, він лише встановлює вимогу щодо того, що дані не можуть зберігатися контролерами безстроково і безцільно.

Вже цитована мною вище британська юридична компанія пише про необхідність врахування певних факторів при обранні строків зберігання та обробки персональних даних. Зокрема, до таких критеріїв відносяться стійкість відносин між контролерами та суб'єктами даних для яких збираються ці дані, природа таких даних, витрати та ризик пов'язані зі збереженням таких даних та нормативні вимоги.[10]

Як ми бачимо з цих запропонованих критеріїв, ми не можемо запропонувати один точний строк щодо всіх даних, адже зрозумілим залишається, що компанія може отримувати різні за тематикою дані та різний їх об'єм і єдиний строк об'єктивно не зможе забезпечити можливість досягнення цілей обробки даних.

Крім того, щодо цього принципу, як і щодо «purpose limitations» діють винятки щодо можливості обробки даних для задоволення суспільних потреб, історичних чи наукових досліджень та статистичних цілей без обмеження на

терміни. Тобто для цих цілей вказані критерії не діють, хоча в той же час, контролери повинні надавати таким даним належних засобів захисту.

Так само щодо захисту передбачено останній принцип, вказаний у ч. 1 ст. 5 GDPR – «integrity and confidentiality». Цей принцип повинен захищати дані індивідів при їх обробці контролерами від несанкціонованого втручання третіх осіб. Комплексно до цього принципу підходить ICO, який у своїх рекомендаціях пише про те, що контролери даних повинні аналізувати ризики пов'язанні зі зберіганням даних, мати внутрішні політики по інформаційній безпеці, шифрувати дані, які знаходяться в них на обробці та гарантувати, що інші контролери чи оператори даних, яким такий контролер передає дані, здійснюють так само належні заходи для збереження даних.[12]

В той же час, критерій належних заходів, на мій погляд, є достатньо оціночним судженням, яке можна звести до звичної презумпції про те, що якщо відбувся несанкціонований доступ до них або їх витік, втрата чи пошкодження, то це вже буде свідчити про те, що дані зберігалися неналежним чином.

Останнім принципом, який передбачений GDPR є «accountability». Він покладає на контролерів зобов'язання «відповідати попереднім принципам та мати можливість це довести»[3]. Як і щодо всіх інших принципів не встановлено критеріїв, як саме контролери повинні мати здатність продемонструвати це. Ірландський наглядовий орган про необхідність наявності цілого комплексу заходів, які дозволятимуть контролеру підтверджувати дотримання контролерами принципів GDPR. Зокрема, до них можна віднести впровадження технічних та організаційних заходів, імплементація чітких і зрозумілих політик по обробці даних, кодексів поведінки, призначення DPO, чіткі умови в договорах з контрагентами щодо захисту персональних даних.[7] Джеральдін Строубрідж також пише про вказані критерії та, окрім них додає про необхідність «оцінки поточної практики, запровадження процедури інвентаризації даних, отримання згоди, яка необхідна для обробки даних, проведення оцінки щодо захисту персональних даних» [6].

З цього зрозуміло, що дотримання контролерами даних принципу «accountability», як і інших принципів захисту за GDPR, завжди буде розглядатися з огляду на конкретні обставини в кожній ситуації окремо.

Описані вище принципи GDPR є основною для всього механізму захисту персональних даних, він повністю побудований на них і не може функціонувати без них. Це обґрунтовує детальність аналізу цих принципів наглядовими органами різних країн ЄС та видання своїх рекомендації щодо дотримання цих принципів.

Водночас так само принципи є найбільш поширеною нормою при правозастосуванні GDPR та найчастіше зустрічаються при виявленні наглядовими органами порушень у сфері захисту персональних даних. Все це дозволяє стверджувати про їх центральне місце у сфері захисту персональних даних.

Крім того, також хотів би звернути увагу на гнучкість цих принципів і відсутність чітких критеріїв. Такий підхід робить GDPR достатньо мобільним та більш пристосованим до змін і трансформації, які властиві сфері захисту персональних даних.

1.1.2 Вимоги до контролюючих органів та їх повноваження за GDPR

Разом зі змінами щодо стандартів захисту персональних даних, які відбулися при впровадженні GDRP, повинні були змінитися і підходи до повноважень контролюючих органів та характер їх взаємодії з контролерами і операторами даних. Такі зміни об’єктивно зумовлені обсягом повноважень, які покладаються на контролюючі органи відповідно до GDPR.

Правове регулювання наглядових органів поділено в GDPR на дві частини – положення щодо формування та щодо компетенції наглядових органів. Частина положень посилається на національне законодавство держав-членів та залишає розв’язання певних питань на розсуд національних законодавчих органів.

Водночас закріплені в GDPR положення охоплюють загальні вимоги до контролюючих органів.

Відповідно до положень GDPR кожна держава-член формує власні наглядові органи з питань захисту персональних даних. Регламент не обмежує країни ні в кількості наглядових органів, ні у механізмі їх взаємодії, встановлюючи лише вимоги щодо того, що наглядовий орган повинен бути створений та визначено механізм взаємодії з іншими наглядовими органами [3].

Сама Європейська комісія визначає data protection authorities як «незалежний державний орган, який здійснює нагляд, за допомогою повноважень щодо розслідування та уточнення застосування закону про захист персональних даних»[13].

Така визначення є досить загальним, відповідно дозволяє країнам розбудовувати структуру органів захисту персональних даних на власний розсуд і ділити повноваження між ними. Водночас в ч. 3 ст. 51 GDPR, визначає, що для взаємодії з органами ЄС, кожна «держава-член призначає наглядовий орган, що повинен представляти такі органи в Раді, та встановлює механізми забезпечення дотримання іншими органами правил механізму послідовності»[3]. Під механізмом послідовності варто розглядати встановлену GDPR вимогу щодо послідовного застосування GDPR в ЄС та співпраці з іншими наглядовими органами [3].

GDPR встановлює єдину вимогу до наглядових органів держав-членів – незалежність. Для досягнення цього положення GDPR встановлюють, як вимоги щодо відсутності будь-якого впливу та положення щодо несумісності діяльності в наглядовому органі з іншою діяльністю, так і вимоги щодо технічного, фінансового забезпечення та формування персоналу наглядових органів [3].

Lydia F. de la Torre у своїй статті розкриває критерій незалежності, опираючись на судову практику Суду ЄС і визначає три основні аспекти цього поняття:

- «Державний контроль за діяльністю наглядового органу є несумісним з незалежністю;

- Керівники наглядових органів можуть призначатися парламентом або урядом держави; законодавчий орган може визначати повноваження таких органів та покласти на наглядовий орган зобов'язання щодо звітування перед парламентом про свою діяльність;
- Функціональна незалежність … є важливою, але недостатньою умовою. Наглядовий орган повинен бути захищений від будь-якого зовнішнього впливу» [14]

Проте, положення GDRP не повністю узгоджуються з такими критеріями. Наприклад, положення ч. 1 статті 53 GDPR визначає, що члени наглядового органу можуть призначатися не тільки парламентом чи урядом, але і главою держави чи незалежним органом, що матиме такі повноваження згідно з законодавством держави-члена [3]. Це вкотре засвідчує, що гнучкість розуміння певних термінів і відсутність чітких меж для окремих термінів.

Водночас якщо продовжити щодо вимог для окремих членів наглядового органу, то варто відзначити, що вони достатньо схожі з вимогами до data protection officer. Вони не визначають окремих критеріїв, які повинні задовільнятися для можливості певними особами бути призначеними членом наглядового органу. Зокрема, «кожен член наглядового органу повинен мати кваліфікацію, досвід та навички, зокрема у сфері захисту персональних даних, необхідні для виконання покладених на нього обов'язків» [3]. Так само, встановлено зобов'язання щодо збереження професійної таємниці та обмеження щодо мінімальних строків перебування на посаді члена наглядового органу – не менше 4 років [3].

При аналізі положень щодо наглядових органів за GDPR варта аналізу також введена GDPR концепція Lead Supervisory Authority (далі – «керівний наглядовий орган» або «LSA»). Концепція покликана врегулювати неоднозначності, пов'язані з транскордонною передачею персональних даних, тобто ситуацій, коли існує велика ймовірність виникнення конфлікту між

повноваженнями різних наглядових органів, щодо взаємодії з контролером чи оператором персональних даних.

Транскордонне опрацювання, відповідно до п. 23. ч. 1 ст. 4 GDPR це –

- «опрацювання персональних даних, що відбувається у контексті діяльності осідків контролера чи оператора в Союзі у більше ніж одній державі-члені, якщо контролер або оператор мають осідки в більше ніж одній державі-члені;
- опрацювання персональних даних, що здійснюють у контексті діяльності єдиного осідку контролера або оператора в Союзі, але яке істотно впливає чи ймовірно істотно впливатиме на суб'єктів даних у декількох державах-членах» [3].

Водночас поняття «істотно впливає» не визначено GDPR. Європейська комісія вважає, що варто тлумачити цей термін з врахуванням цілого ряду критеріїв, зокрема, при такому тлумаченні варто зважати на контекст, тип даних, мету, можливість настання негативних наслідків чи обмеження прав і свобод індивідів, вплинути на здоров'я, фінансовий стан індивідів, є підставою для дискримінації чи опрацювання проводиться щодо великих обсягів персональних даних [15].

Застосування концепції LSA дозволяє визначати наглядовий орган якої з держав-членів ЄС буде розглядати питання, пов'язані з обробкою персональних даних. Таким чином, контролер чи оператор, який здійснює обробку персональних даних, матиме можливість взаємодіяти лише з наглядовим органом однієї з держав-членів ЄС, незалежно від кількості офісів/представництво, які діють у ЄС.

За умовчанням, повноваження діяти як LSA GDPR покладає на наглядовий орган держави-члена "of the main establishment or of the single establishment"[2].

Водночас, так само GDPR розкриває поняття "main establishment". Зокрема, для контролерів даних "main establishment" може бути утворення в будь-якій організаційно-правовій формі (український переклад GDPR застосовує термін – «осідок»[3]), де знаходиться центральна адміністрація контролера в ЄС

або утворення, що приймало рішення про засоби і цілі обробки персональних даних та може забезпечити виконання цього рішення.[3] Для операторів персональних даних «осідок» буде або утворення, де знаходиться центральна адміністрація або утворення, яке проводить основну частину обробки персональних даних[3].

Як пояснює Guidelines for identifying a controller or processor's lead supervisory authority, така альтернатива при визначені «main establishment» пов'язана з тим, що «повинен бути єдиний керівний наглядовий орган для різноманітних варіантів обробки персональних даних, які проводяться транснаціональними компаніями. Однак існують випадки, коли окремі утворення приймають рішення про цілі і обробку персональних даних автономно від центральної адміністрації» [15].

Параграф 36 GDPR визначає, що «main establishment» варто визначати за «об'єктивними критеріями, з огляду на результативну та фактичну управлінську діяльність, у ході якої ухвалюються ключові рішення щодо цілей та засобів опрацювання на основі стабільних домовленостей» [3]. В той же час GDPR передбачає, що ні місце обробки персональних даних, ні використання наявність технічних засобів не повинні мати вирішального значення [3].

Застосування концепції керівного наглядового органу не означає, що наглядові органи інших країн не повинні аналізувати діяльність окремих утворень контролера чи оператора даних в інших державах-членах ЄС, більше того, відповідно до ст. 60 GDPR керівний наглядовий орган повинен сприяти у діяльності інших наглядових органів, забезпечувати обмін інформацією з ними та залучати до розслідування окремих кейсів порушення GDPR за необхідності. В той же час, керівний наглядовий орган повинен брати до уваги проекти рішень щодо окремих ситуацій, які розробляє наглядовий орган іншої держави-члена[3].

Завдання кожного окремого наглядового органу визначені у статтях 56 GDPR, зокрема до них можна віднести: проведення моніторингу, консультування та сприяння обізнаності громадськості та контролерів і операторів даних щодо положень GDPR, розгляд скарг і т.д. Перелік завдань не

є вичерпним, а їх виконання для суб'єктів даних відбувається на безоплатній основі[3].

Всі повноваження наглядових органів за GDPR, які передбачено статтею 57, поділені на три основні групи: «слідчі, виправні та дозвільні і консультаційні повноваження»[3]. Попри те, що GDPR надає наглядовим органам достатньо широкі повноваження, загалом вони співвідносяться з завданнями покладеними на наглядові органи.

Підсумовуючи, варто зазначити, що положення GDPR в частині наглядових органів віддають на розсуд законодавчих органів держав-членів ЄС, окрім вимог щодо незалежності наглядових органів. Водночас, варто зауважити, що введення GDPR концепції LSA покликано дати більшу визначеність для контролерів та операторів персональних даних та є вдалим варіантом попередження суперечності при транскордонній передачі даних.

1.1.3 Поширеність впливу GDPR з огляду на територіальність його дії

Після прийняття GDPR для країн, які не є членами ЄС, зокрема і для України, стала актуальною тематика застосовності до них положень GDPR. Така зацікавленість пояснюється застосуванням у регламенті відразу кількох критеріїв для визначення його територіальної дії. Зокрема, можна стверджувати про два такі критерії – безпосередньо територіальний та критерій цілісного спрямування [16], який залежить від взаємодії контролерів даних з суб'єктами, які є громадянами ЄС чи знаходяться на території ЄС.

Обидва критерії сформульовані у ст. 3 GDPR. Зокрема, частина перша передбачає, що: «Регламент застосовується до обробки персональних даних, що здійснюється в ході діяльності контролера чи оператора даних в Союзі, незалежно від того чи відбувається така обробка в межах Союзу» [3]. За своєю суттю це територіальний критерій. Хоча цей критерій застосовний лише до суб'єктів, які створенні в ЄС, з його положень зрозуміло, що для GDPR є неважливим місце, де здійснюється власне обробка даних – в межах ЄС чи ні.

Другий критерій сформульовано одразу кількома положеннями. Частина друга статті 3 GDPR передбачає, що: «Регламент буде застосовний до обробки даних суб'єкт яких знаходиться в Союзі… коли діяльність пов’язана з:

пропозицією (*а не з «постачанням», як зазначено в офіційному українському перекладі – прим. Дейнека Євгеній*) товарів чи послуг, незалежно від того чи вимагається за них плата;

моніторингом поведінки суб’єктів, допоки така поведінка здійснюється в Союзі» [2].

Крім того, регламент буде застосовуватися, якщо «буде застосовуватися законодавство держави-члена ЄС» [2].

Такі положення в цілісності формулюють критерій цілісного спрямування, який і робить актуальним GDPR для інших країн ЄС. Це своєрідне нав’язування стандартів змусило виконувати положення GDPR, як мінімум контролерів даних, які мають тісні зв’язки з ЄС.

Водночас від початку зав’язалася полемічна дискусія серед науковців і практиків права щодо меж застосування цих положень. Здебільшого, вона зводилася до питання меж застосування територіальної дії GDPR. Українські правники так само приділяють цьому увагу.

Зокрема, аспекти територіальної дії GDPR розкриваються у статті Арсена Кулька. Так він наводить кілька прикладів, коли положення GDPR будуть та не будуть застосовуватися до компаній. Я не готовий погодитися з усіма висновками А. Кулька, проте аналізуючи його роботу можна зробити висновок про те, що застосування GDPR на практиці, буде залежати від місця реєстрації вебсайту та доменних імен, наявності різних мовних версій вебсайту, валюти розрахунків, наявності офісів/філій в країнах ЄС або наявності інших об’єктів дозволятимуть співвіднести їх з певним суб’єктом (наприклад, місце на сервері, яке буде орендувати компанія), наявності чіткої цільової аудиторії, яка зацікавлена в придбанні товарів чи послуг компанії [17].

Однак А. Кулик розглядає окремі випадки та не намагається знайти конкретні критерії, які дозволяли б визначати, чи підпадає діяльність окремих суб'єктів під дію GDPR.

Британська компанія Ashurst у своїй статті щодо територіальної дії GDPR з посиланням на Guidelines 3/2018 on the territorial scope of the GDPR, пише про те, що «рекомендовано застосовувати наступні три підходи до оцінки застосовності положень статті 3(1) GDPR до процесу обробки персональних даних:

- Наявність представництва компанії в ЄС;
- Чи відбувається обробка «в межах діяльності» компанії;
- Застосовність вказаної статті за наявності представництва незалежно від місця обробки даних» [18]

Перш за все більша визначеність цих критеріїв дозволяє краще класифікувати застосовність критеріїв обробки даних в окремих ситуаціях. Крім того, це наштовхує на думку про те, що нормативно-правовим актам ЄС властиві досить коротко сформульовані норми у нормативно-правових актах і величезні Guidelines, які розкривають деталі норми.

Більше того, з мого аналізу вказаних Guidelines, стає зрозумілим, що вони, у великій частині, побудовані на наявній судовій практиці. Таким чином, можна стверджувати, що Guidelines видаються вже через певний час після початку дії нормативно-правового акту, стаючи результатом вже наявної практики застосування правових норм. Так, зокрема, Guidelines 3/2018 on the territorial scope of the GDPR було затверджено вже у 2019 році, через півтора року після того, яка GDPR почав діяти.

Так само, Guidelines містить пояснення і до вимог, що стосуються цілісного спрямування. Як і щодо територіального критерію EDPB рекомендує застосування відразу двох критеріїв: «визначити, що обробка даних стосується персональних даних суб’єктів, які знаходяться в Союзі та … чи стосується така обробка пропозиції товарів чи послуг або моніторингу поведінки» [19].

Відразу варто зауважити, що параграф 14 GDPR наголошує на тому, що: «Захист, передбачений цим Регламентом, поширюється на фізичних осіб, незалежно від їхнього громадянства чи місця проживання, під час опрацювання їхніх персональних даних» [3].

Тобто неважливою є наявність в осіб громадянства ЄС, важливим, в контексті даного критерію, є факт обробки персональних даних особи, яка перебуває на території ЄС.

Водночас, EDPB звужує категорію осіб, обробка даних щодо яких підпадає під GDPR. Зокрема, EDPB передбачає, що «якщо відбувається пропозиція послуг для індивідів за межами ЄС і послуги не перестають надаватися, коли індивід в'їжджає на територію ЄС, обробка даних, пов'язана з процесом надання цих послуг, не буде підпадати під правила GDPR»[19].

Більшої деталізації зазнає і додатковий критерій щодо «пропонування товарів та послуг та моніторингу поведінки»[3]. Зокрема, одним із ключових моментів EDPB вважає «демонстрацію контролером наміру запропонувати товари чи послуги суб'єкту даних, який знаходиться в межах ЄС» [19]. Базуючись на власних судженнях та наявній практиці Суду Справедливості ЄС, EDPB надає цілий ряд факторів, які можуть свідчити про наміри контролера надавати товари/послуги суб'єктам в ЄС: «ЄС або держава-член згадуються при описі товару чи послуги; оплата послуг провайдерів в ЄС; маркетингові кампанії контролера в державах членах ЄС; міжнародний характер діяльності; контакти контролера для зв'язку в межах ЄС; доменне ім'я; опис поїздок по державах-членах ЄС; згадка про міжнародних користувачів; мова чи валюта; пропозиція доставки в ЄС» [19].

Тобто при вирішенні чи повинна підпадати обробка персональних даних під дію GDPR, необхідно враховувати великий перелік критеріїв, який не є виключним, що залишає остаточне розв'язання питання на дискреції суб'єктів, що застосовують GDPR - як контролерів, так і наглядових органів держав-членів ЄС.

Інший критерій, який може бути наявний для застосування GDPR за «цільовим спрямуванням», це «monitoring of data subjects' behaviour» [19]. Найважливішим тут, на мій погляд, є визначення поняття «моніторинг». В параграфі 24 GDPR міститься пояснення, яке визначає, що для визнання обробки персональних даних моніторингом «необхідно встановити, чи є фізичні особи об'єктами відстежування в Інтернеті, у тому числі чи може мати місце подальше використання методик опрацювання персональних даних, що складають з профайлінгу фізичної особи, зокрема для прийняття рішення щодо неї або нього чи для проведення аналізу, або передбачення її або його особистих переваг, поведінки чи ставлення» [3]. З вказаним не погоджується EDPB, яка пише про те, що «відстеження через інші типи мережі чи технології, з одночасною обробкою персональних даних, повинні братися до уваги при визначенні наявності в такій обробці моніторингу поведінки»[19]. Так, до заходів, що можуть свідчити про моніторинг поведінки EDPB включає також: «поведінкову рекламу; відслідковування геолокації; відстежування з використанням cookie-файлів; послуг з аналізу дієти та здоров'я особи, що надаються онлайн; відеоспостереження; маркетингові дослідження ринку; регулярний моніторинг стану здоров'я» [19]

Таким чином, зрозуміло, що для моніторингу поведінки, як і для наявності наміру щодо пропозиції товарів чи послуг, існує невичерпний перелік критеріїв, які можуть свідчити про наміри контролера даних здійснювати моніторинг поведінки суб'єктів даних.

Ще одним важливим нововведенням GDRP щодо стандартів захисту персональних даних є вимоги щодо наявності представників у ЄС, для компаній, які мають намір обробляти або обробляють персональні дані, і підпадають під дію GDPR.

Сергій Богорада пише про те, що: «Положення Регламенту передбачають, що у разі, коли компанія, яка не має осідку на території ЄС, але при цьому діє відповідно до Регламенту, не призначить представника на території ЄС, то така компанія порушує Регламент» [16].

Параграф 80 GDRP передбачає, що: «Представник повинен діяти від імені контролера або оператора, … Представника необхідно чітко призначати на підставі письмового доручення … На призначеного представника поширюється застосування виконавчого провадження у випадку порушень з боку контролера або оператора» [3]. Аналогічні вимоги щодо письмової форми призначення представника містяться і в статті 27 GDPR.

Сергій Богорада також пише про те, що : «представником можуть бути, як фізичні так і юридичні особи, при цьому, головною вимогою залишається підтвердження факту того, що місце реєстрації представника знаходиться на території ЄС … представниками можуть бути юридичні та консалтингові компанії, які виступатимуть представником не лише для однієї компанії»[16]. Натомість EDPB навіть пише, що якщо відбувається: «декілька варіантів обробки даних, які підпадають під дію статті 3 (2) GDPR, … немає потреби призначати кількох представників» [19]. Водночас EDPB наголошує про несумісність між статусом представника та DPO (уповноваженого по захисту персональних даних) [19].

Таким чином, зрозуміло, що вимоги до представників не є надзвичайно високими. Крім письмової угоди та наявності реєстрації такого представника в ЄС, GDPR не висуває додаткових умов, які повинні задовольняти такі представники. Натомість стаття 27 GDPR містить кілька випадків, коли обробка персональних даних не потребуватиме призначення представника в ЄС. Зокрема до таких випадків належать:

- Опрацювання персональних даних органами публічної влади;
- Одиничні випадки обробки персональних даних;
- Неопрацювання даних у великих обсягах;
- Неопрацювання специфічних категорій;
- Неопрацювання даних щодо судимостей;
- Не призводить до виникнення ризику для прав і свобод фізичних осіб [3].

З огляду на вищесказане, з’ясовано, що територіальна дія GDPR за час правозастосування цього нормативно-правового акту уточнювалася і кристалізувалася. На сьогодні існує достатньо критеріїв та роз’яснень, які дозволяють аргументувати застосування чи не застосування GDPR до окремих категорій випадків. В той же час, територіальна дія GDPR залишається достатньо гнучкою і стає першочерговим критерієм для контролерів при взаємодії з GDPR.

1.1.4 Відповідальність за порушення вимог щодо обробки персональних даних за GDPR

Відповідальність, яка може наставати за порушення норм та вимог GDPR була і залишається однією з найбільш резонансних тем, які стосуються GDPR. Особливо яскраво це виявляється в українському правовому середовищі, яке починало знайомитися з GDPR через розміри штрафів, які ним передбачено.

Така резонансність є зрозумілою, тому що розміри штрафів, які GDPR дозволяє накладати на контролерів та операторів даних є об’єктивно великими та різко резонують з штрафами, які встановлюються попередніми нормативно-правовими актами.

Варто відразу зазначити, що штраф це не єдиний із видів юридичної відповідальності, який може бути застосований до контролерів і операторів. В одному з інтерв’ю для видання Reuters Джованні Буттареллі (European Data Protection Supervisor) говорив: «Я очікую, що перші штрафи GDPR за деякі випадки будуть до кінця року. Не обов’язково штрафи, а також рішення закликати контролерів, накласти попередню заборону, тимчасову заборону або поставити їм ультиматум»[20].

Тобто штрафи варто розглядати, як останній, найсуворіший захід, який повинен застосовуватися до контролерів даних. Частина 2 статті 83 GDPR передбачає можливість накладення штрафів «як доповнення до, чи замість, заходів, вказаних у пунктах (a)-(h) і (j) статті 58(2)»[3]. Саме положення статті 58(2) покладають на наглядові органи «виправні повноваження» щодо

надсилання попереджень, доган, встановлення обмежень чи заборон на обробку персональних даних і т.д. [3].

Варто також зазначити, що паралельно зі штрафами та іншими заходами впливу, контролери та оператори даних повинні відшкодувати шкоду суб'єктам даних, яким завдано шкоду. Тут хотів би відмітити, що «будь-який контролер, залучений до опрацювання, несе відповідальність за шкоду, заподіяну опрацюванням, що порушує положення Регламенту. Оператор несе відповідальність за шкоду, заподіяну опрацюванням лише тоді, коли він не дотримується обов'язків за Регламентом, спрямованих безпосередньо на оператора, або якщо він діє поза чи всупереч законним вказівкам контролера»[3].

Тобто відповідальність оператора достатньо обмежена, вона може наступати якщо буде доведено, що він діє всупереч вказівкам контролера, що на мою думку, не зовсім просто або якщо певні вимоги до операторів передбачені безпосередньо щодо операторів самим GDPR. Для порівняння варто зауважити, що положень GDPR, які стосуються операторів даних набагато менше, ніж для контролерів даних. Тому, можна сказати, відповідальність операторів даних обмежена певними умовами, які звужують застосування до них заходів впливу.

Аналогічні обмеження та відповідальність покладаються на субоператорів даних, зокрема ICO пише: «якщо ви є субоператором, ви будете нести відповідальність за будь-яку шкоду, заподіяну обробкою, лише якщо ви не виконали британські GDPR-зобов'язання, покладені на процесори, або діяли всупереч законним інструкціям контролера, переданим процесором, щодо обробки» [21].

Штрафні санкції за GDPR так само не є однозначними. Частини 4 і 5 статті 83 GDPR передбачають два види штрафів залежно від сутності порушення – 10 млн євро чи 2% загального глобального річного обігу або 20 млн євро чи 4% загального глобального річного обігу, в обох випадках застосовується більша сума [3].

Водночас Сергій Богорада у своїй статті наводить приклади кейсів, коли компанії отримували штрафи зовсім різних розмірів. Він наводить приклад

австрійського підприємства, яке було оштрафоване на 4 000 Євро, португальської клініки, яку оштрафовано на 400 000 Євро та британської компанії, яку оштрафовано на 17 млн фунтів [22].

Варто відзначити, що така диференціація не є винятком. Міжнародна юридична компанія CMS підготувала і оновлює GDPR Enforcement Tracker, який являє собою базу даних з інформацією про всі кейси пов'язані з діяльністю GDPR. Трекер містить інформацію про різноманітні кейси від 28 Євро до понад 50 млн Євро (обидва приклади наведених кейсів стосуються різних компаній корпорації Google)[23]. Це свідчить про те, що штрафи за GDPR можуть мати велику диференціацію і необов'язково повинні бути надзвичайно великими для компаній.

Така диференціація обґрунтована наявністю в GDPR переліку обставин, які повинні бути проаналізовані наглядовими органами при розв'язання питання щодо накладення штрафів на контролера чи обробника даних. Оксана Духовна к своїй статті пише про сім таких критеріїв, зокрема:

- «Характер, тяжкість і тривалість порушення, враховуючи характер, обсяг або мету обробки. Кількість постраждалих суб'єктів даних та розмір завданої шкоди;
- Навмисний чи ненавмисний характер порушення;
- Будь-які дії, вжиті контролером чи процесором для зменшення шкоди, завданої суб'єктам даних;
- Ступінь відповідальності контролера чи процесора, враховуючи вжиті ними технічні та організаційні заходи згідно з Регламентом;
- Будь-які релевантні попередні порушення з боку контролера чи процесора;
- Ступінь співпраці з наглядовими органами з метою усунення порушення або пом'якшення можливих негативних наслідків порушення;

- Категорії персональних даних, які постраждали в результаті порушення» [24]

На додачу до вказаних обставин цей перелік варто доповнити кількома обставинами: «спосіб, у який наглядовому органу стали відомо про порушення …; якщо заходи, вказані в статті 58(2), було раніше призначено проти відповідного контролера або оператора …; дотримання затверджених кодексів поведінки» [3].

Варто заувчажити, що такий перелік не є виключним. Пункт (k) ч. 2 ст. 83 дозволяє наглядовим органам враховувати будь-які інші фактори при прийнятті рішень [3]. Тобто визначення остаточного розміру штрафів залишається дискреційними повноваженнями наглядових органів держав-членів ЄС.

Крім того, GDPR дозволяє державам-членам встановлювати «правила щодо інших санкцій, застосовних до порушень цього Регламенту, зокрема, за порушення, що не підлягають накладенню адміністративних штрафів відповідно до статті 83» [3]. Таким чином, бачимо, що й у випадку з накладенням штрафів GDPR залишає багато питань на розсуд держав-членів та їх наглядових органів.

Крім безпосередньо заходів юридичної відповідальності, так само юристи-практики наголошують на непрямих наслідках порушення положень GDPR. Зокрема, у літературі є різні додаткові можливі наслідки, зокрема: «репутаційні збитки, … витрати пов’язані з аналізом та контролем за завданими збитками, … відкликання сертифікації, … заборона на обробку, … відповідальність за збитки» [25].

Таким чином, варто зауважити, що механізм притягнення до відповідальності, який прописаний в GDPR, містить цілий спектр заходів впливу і не обмежується виключно накладенням штрафів.

Більше того, наглядові органи за GDPR мають широкі повноваження щодо розслідування та накладення штрафів, що крім всього іншого включають дискреційні повноваження щодо визначення розмірів штрафів, які мають забезпечити належну превентивність заходів впливу. Водночас це зумовлює

наявність на практиці значно менших штрафів, які накладаються на контролерів та операторів даних.

1.2 Діяльність контролюючих органів захисту персональних даних у ЄС

Структура органів ЄС у галузях, які знаходяться у сфері компетенції Європейського Союзу, характеризується наявністю окремих органів, які функціонують на наднаціональному рівні. Захист персональних даних належить до сфер, які регламентуються та врегульовуються на рівні Європейського Союзу. Про це свідчить, положення статті 39 Договору про Європейський Союз[26] та статті 16 Договору про функціонування Європейського Союзу [27].

З огляду на це, при здійсненні аналізу правових засад і особливостей діяльності наглядових органів окремих держав-членів ЄС, першочергово важливими є особливості діяльності органів, які діють на наднаціональному рівні. Їх аналіз дозволить з'ясувати окремі аспекти їх взаємодії з іншими органами в ЄС та проаналізувати дотримання механізму послідовності, передбаченого ст. 63 GDPR [3].

В межах ЄС немає єдиного органу, діяльність якого безпосередньо спрямована на захист персональних даних. Одночасно існує кілька органів, повноваження яких, повністю чи частково, пов'язані з регулюванням питань, які стосуються захисту персональних даних в ЄС. Серед цих органів, можна виокремити – Європейську комісію, Європейську раду із захисту даних, яка була заснована самим GDPR [3] та Європейського інспектора із захисту даних.

Європейська комісія «наділена найбільшими виконавчими повноваженнями»[28] в ЄС. Зокрема, їй належить «виключне право ініціювати прийняття законодавчих актів ЄС» [28]. Безпосередньо, Комісія не набуває нових повноважень за GDPR. Водночас GDPR передбачає окремі аспекти взаємодії між Комісією та European Data Protection Board (далі - "**EDPB**"). Зокрема, Комісія може подавати запити до EDPB, в той час, як EDPB повинна сповіщати Комісію про затримки в їх розгляді та випадки застосування екстреної

процедури, коли не дотримується механізм послідовності. Крім того, EDPB консультує Комісію з питань захисту персональних даних та готує звіти про стан захисту персональних даних, який подається в тому числі і Європейській комісії [3].

В той же час, на Комісію покладено повноваження «ухвалювати імплементаційні акти загальної сфери дії для того, щоб визначити домовленості щодо обміну інформацією між наглядовими органами та наглядовими органами і Радою» [3]. З цього слідує, що повноваження Європейської Комісії за GDPR мають наглядовий та управлінський характер.

Центральне місце у системі органів, діяльність яких спрямована на нагляд за захистом персональних даних займає – EDPB. Сам орган позиціонує себе як «незалежний європейський орган, який сприяє послідовному застосуванню правил захисту персональних даних у Європейському союзі та сприяє співпраці між органами ЄС із захисту даних» [29].

Створення цього органу передбачено безпосередньо в GDPR і формування відбувається за рахунок керівників чи представників наглядових органів всіх держав-членів ЄС (по одному з кожної держави) та Європейського інспектора із захисту даних [3]. Важливо також, що як і наглядові органи держав-членів, EDPB повинна залишатися незалежною: «Рада, під час виконання своїх повноважень, не повинна запитувати чи приймати вказівки від будь-якої особи» [3]. Єдиним обмеженням незалежності в такому випадку, можуть виступати взаємини з Європейською Комісією при поданні запитів до EDPB. Крім того, незалежність EDPB не обмежує факту підзвітності EDPB іншим органам ЄС – Комісії, Європарламенту та Раді ЄС.

Варто зауважити, що EDPB не є звичайним наглядовим органом, який відрізняється від інших наглядових органів держав-членів ЄС лише поширеністю своїх повноважень на всю територію ЄС. Повноваження EDPB включають: «надання загальних вказівок (включаючи guidelines, рекомендації та кращу практику) для роз'яснення; прийняття висновків щодо узгодженості, покликаних забезпечити послідовне тлумачення GDPR усіма національними

наглядовими органами… ; консультування Європейської комісії з питань захисту даних та нового законодавства ЄС, що має значення для захисту персональних даних»[30]. Так само, EDPB уповноважена забезпечувати дотримання механізмів послідовності, надавати свої висновки щодо окремих ситуацій та може вирішувати певні спори пов'язані з порушенням захисту персональних даних.

Для забезпечення належної роботи EDPB, створюється Секретаріат. Його основне призначення – забезпечення нормального функціонування EDPB, що полягає у тому, що він «надає аналітичну, адміністративну та логістичну підтримку Раді»[3]. Передбачення подібних положень в GDPR як для EDPB, так і для наглядових органів держав-членів ЄС, є ще однією з гарантій незалежності EPDB та інших наглядових органів та послідовності GDPR у контролі за дотриманням цих вимог.

Стаття 75 GDPR, зокрема передбачає, що Секретаріат EDPB формується Європейським інспектором із захисту персональних даних – European Data Protection Supervisor [3]. Хоча запровадження такої посадової особи випливає ще з положень Договору про функціонування Європейського Союзу, зокрема статті 16, яка передбачає регламентацію та контроль за захистом персональних даних [27] і донедавна його діяльність регламентувалася Регламентом 45/2001 [31], поточна детальна регламентація його діяльності, передбачена у відносно новому Регламенті ЄС № 2018/1725 від 23 жовтня 2018 року.

Регламент передбачає, що «Європарламент та Рада ЄС призначають Європейського інспектора із захисту персональних даних за спільною згодою строком на 5 років на підставі списку, що формується Єврокомісією за результатами публічного обговорення кандидатів»[31].

EDPS входить до складу EDPB за своєю посадою, що передбачено статтею 68 GDPR [3]. Крім того, мета його появи і призначення співзвучні з EDPB і пов'язані, із захистом персональних даних в межах ЄС. Основні завдання EDPS можна окреслити наступним чином:

«моніторинг та забезпечення захисту персональних даних та конфіденційності при обробці таких даних установами та органами ЄС; надання консультацій установам та органам ЄС з усіх питань, пов'язаних з обробкою персональних даних…; моніторинг технологій, що можуть мати вплив на захист персональних даних; залучення Судом ЄС для надання експертних висновків щодо тлумачення законодавства про захист персональних даних; співпраця з наглядовими органами держав-членів щодо покращення механізму послідовності захисту персональних даних» [32]

Попри достатню схожість у повноваженнях та завданнях в EDPS та EDPB не можна стверджувати про їх ідентичність. Так, діяльність EPDS чітко спрямована на контроль за обробкою персональних даних органами ЄС, в той час, як EDPB має, в тому числі повноваження щодо вирішення суперечливих ситуацій при застосуванні положень GDPR та вирішення складних спорів між наглядовими органами держав-членів ЄС.

Крім того, окремі положення GDPR так само, розмежовують і формують правила співіснування між EDPS та EDPB. Так, параграф 139 GDPR передбачає, що EDPS «повинен мати особливе право голосу» [3] при прийнятті рішень EDPB.

З проаналізованого, можна сказати, що система органів захисту персональних даних на рівні ЄС є розмежованою та має горизонтальну та вертикальну ієрархію. Водночас повноваження та ресурси окремих органів ЄС є чітко визначеними та дозволяють їм діяти абсолютно незалежно один від одного. Так само, є чітко визначені процедури та механізми, які дозволяють вирішувати суперечності при взаємодії органів ЄС та наглядових органів держав-членів та цих наглядових органів між собою.

1.3 Особливості імплементації положень GDRP в окремих країнах Європи

1.3.1 Велика Британія

Аналіз механізмів захисту окремих держав-членів ЄС обумовлений необхідністю дослідження особливостей захисту персональних даних в державах-членах. Оскільки, GDPR залишає деякі питання або сфери для вирішення на рівні національного законодавства, аналіз такого законодавства держав-членів ЄС допоможе більш якісно підійти до аналізу практики застосування GDPR окремими наглядовими органами.

Перелік країн сформований на основі об'ємів практики правозастосування GDPR наглядовими органами окремих країн. Водночас аналіз особливостей у Великій Британії обумовлено відразу кількома критеріями.

Перш за все, наглядові органи Великої Британії відомі кількома гучними кейсами щодо дотримання норм GDPR – Marriott International Inc, British Airways [23] та Aggregate IQ [24]. Варто також зауважити, що штрафи накладені ICO в рамках цих справ належать до переліку найбільших штрафів наглядових органів (штрафи Marriott та British Airways) [33], а за загальною сумою штрафів Велика Британія є четвертою серед країн ЄС, при тому, що штраф як санкцію ICO застосовує набагато рідше, ніж в Німеччині, Італії чи Іспанії [33].

Крім того, в ході проведеного аналізу в рамках попередньої частини роботи, можу сказати, що захист персональних даних у Великій Британії та діяльність ICO суттєво відрізняється від інших держав-членів ЄС наявністю великої кількості власних роз'яснень та рекомендацій. І це не дивлячись на те, що Велика Британія вийшла з Європейського Союзу і на момент написання цієї роботи вже закінчився перехідний період протягом якого законодавство ЄС, в тому числі і GDPR, продовжували діяти на території Великої Британії.

Законодавство Великої Британії, яке регулює захист персональних даних було змінено водночас з набранням чинності GDPR та адаптоване до його нововведень [34]. Закон про захист даних (англ. – "Data protection act", далі - "**DPA**") містить досить схожі, іноді навіть аналогічні, положення до GDPR. Так, наприклад, ст. 207 DPA, якою врегульовано його територіальну дію, має два аналогічні критерії для застосування DPA – територіальний і критерій цілісного спрямування [35].

Водночас сфера його правового регулювання є ширшою за сферу регулювання GDPR. Окремий, третій розділ DPA передбачений для регулювання: «обробки персональних даних у процесі діяльності, яка виходить за рамки законодавства Європейського Союзу» [35]. Так, наприклад, DPA застосовується до обробки персональних даних публічними установами в рамках FOI.

Водночас DPA не є єдиним нормативним документом, який регулює сферу обігу персональних даних у Великій Британії. На сьогодні, продовжує діяти Privacy and Electronic Communications Regulations (PECR). Застосування цього акту обмежується окремими сферами, зокрема: «електронним маркетингом, застосуванням «cookies» чи споріднених програм, державними послугами зв'язку та конфіденційністю осіб при використанні мереж зв'язку» [36]

PERC не походить від GDPR, а базується на більш ранньому нормативному документі – Директиві 2002/58/ЄС [36]. З огляду на це, його правозастосування є абсолютно незалежним ні від DPA, ні від GDPR і має відбуватися паралельно з вказаними нормативними актами [36].

Крім того, у зв'язку з закінченням перехідного періоду, GDPR втрачав свою силу для Великої Британії з 1 січня 2021 року. Відповідно, йому на зміну прийшов так званий «UK GDPR» [37]. Цей нормативний акт «визначає ключові принципи, права та обов'язки щодо більшої частини сфер обробки персональних даних у Великій Британії, крім обробки персональних даних правоохоронними та розвідувальними органами» [37].

З огляду на ці нормативні акти, стає зрозуміло, що після закінчення перехідного періоду контролери та оператори даних у Великій Британії повинні дотримуватися вимог PERC, DPA, UK GDPR. Водночас з огляду на територіальну дію GDPR, а саме на критерій цілісного спрямування, контролери та оператори даних, діяльність яких буде направлена на суб'єктів даних з ЄС, повинні будуть дотримуватися і GDPR також.

Наглядовий орган Великої Британії у сфері захисту персональних даних - ICO. DPA, зокрема стаття 115 передбачає, що на ICO «покладаються функції

передбачені ст. 57 (Завдання) та 58 (Повноваження) GDPR, а також інші обов'язки передбачені Розділом 2» [35]. З цього слідує, що структура органів захисту персональних даних у Великій Британії не є розгалуженою, вона включає лише ICO, який водночас має три територіальні підрозділи в різних частинах королівства – Шотландії, Уельсі на Північній Ірландії [38].

Водночас ICO широко співпрацює з наглядовими органами інших країн через підписання Меморандумів про взаєморозуміння (Memorandum of Understanding), останній з яких було підписано з Філіппінами у січні 2021 року [39].

1.3.2 Іспанія

На даний момент, Іспанії залишається лідером за кількістю розглянутих кейсів. За підрахунками CMS, їх на цей час 173 [23]. Крім того, іспанські наглядові органи 158 разів накладали штрафи [33] на суб'єктів, що здійснюють обробку персональних даних, що дозволяє Іспанії бути лідером за цим показником, випереджаючи інші держави-члени ЄС.

Водночас іспанські наглядові органи є досить ліберальними і їм не властиво накладати великі суми штрафів, незалежно від розмірів порушника чи тяжкості порушення. Найбільший відомий мені штраф – 6 000 000 Євро, який було накладено на фінансову компанію Caixabank SA [23].

Законодавство Іспанії у сфері захисту персональних даних, як і законодавство Великої Британії, зазнало змін і було приведено у відповідність з GDPR. Водночас основний закон Іспанії – Organic Law 3/2018, у цій сфері не є вичерпним джерелом та не застосовується до всіх сфер обробки персональних даних. Цей Закон, який набрав чинності в грудні 2018 року, зосереджується на п'яти питаннях: «меті закону про захист персональних даних, розширення прав при обробці даних, Data protection officer, обробка персональних даних політичними партіями та цифрові права у сфері працевлаштування»[40].

Крім того, Закон 3/2018 встановлює окремі положення, які відрізняються від положень GDPR. Так, наприклад, віковий критерій для можливості надання згоди неповнолітнім на обробку персональних даних встановлено на рівні 14 років [41], в той час, як GDPR встановлює мінімальний вік – 16 років.[3]

Так само, Закон 3/2018 встановлює «впроваджує систему реєстрації «внутрішніх скарг» (тобто системи, яка дозволяє повідомляти про порушення), яка дозволяє подавати анонімні скарги» [41]. Варто зауважити, що GDPR оминає питання можливості подання анонімних скарг. Ймовірно, це обґрунтовано неоднозначністю і різним ставленням до правильності опрацювання скарг, які є анонімними.

Як вже зазначалося вище, великою увагою в законі наділені цифрові права. Так, законом передбачені цілий ряд прав суб'єктів даних пов'язаних з їх активністю в мережі Інтернет. Зокрема, сюди відносять: «право на інтернет нейтральність та універсальність доступу до інтернету; цифрову безпеку; цифрову освіту; на конфіденційність при використанні пристроїв на робочому місці; захист дітей при використанні інтернету; право бути забутим під час пошуків в інтернеті та у соціальних мережах» [42].

Крім того, ряд інших сфер, де відбувається обробка персональних даних, мають додаткове чи повністю окреме правове регулювання. До цих сфер належать, зокрема: конфіденційність персональних даних в сімейних відносинах, обробка персональних даних судами, електронна комерція, охорона здоров'я та сфера фінансових послуг [43].

Іспанія, так само як і Велика Британія, має єдиний наглядовий орган, що контролює захист персональних даних – Agencia Espanila Protetion Datos (далі – «**AEPD**»)[44]. В свою чергу, наглядовий орган має структурні підрозділи в окремих автономних регіонах Іспанії – Каталонії, Андалусії та країні Басків [44]. Такі органи володіють певною автономією при розгляді конкретних кейсів щодо обробки персональних даних, що стосуються їх регіонів [44].

Варто зауважити, що AEPD є не тільки наглядовим який має одну з найбільшої кількості зафіксованих порушень [33], але достатньо активно

просуває нові підходи до обробки персональних даних та оновлює підходи до окремих категорій цій сфери. Так, наприклад, великої уваги набули зміни AEPD щодо використання компаніями cookie-файлів. Такі зміни були прийняті у 2020 році та пов'язані зі схожими змінами від EDPB [45].

Самі по собі cookie-файли – це «текстові файли, що зберігаються на пристрої користувача, в той час, як здійснюється навігація по вебсайту. Такі файли використовуються для збору персональних даних» [46]. Оновлення в рекомендаціях AEPD, зокрема стосуються надання згоди суб'єктами даних на використання cookie та можливості альтернативних варіантів перегляду вебсайтів [45]. Так само AEPD, одним із перших, ще 12 березня 2020 року, наглядових органів ЄС зробив свої заяви щодо особливостей обробки персональних даних в період пандемії COVID-19 [47] - керівні рекомендації щодо: «правових основ для обробки персональних даних та мінімізації даних» [47].

З огляду, на вищевказане, слід зробити висновок, що Іспанія має достатньою широку та розгалужену законодавчу базу сфері персональних даних, яка збалансовано регулює обробку персональних даних в окремих сферах. Крім того, іспанський захист персональних даних можна схарактеризувати, як легко адаптований до змін у сучасного світу.

1.3.3 Італія

Італія, як й інші країни, досліджені в межах цього розділу, є однією з передових держав щодо розгляду кейсів пов'язаних з GDPR. В той же час Італія є лідером за сумою коштів, які були сплачені, як штрафи за порушення положень GDPR [33]. Це обумовлено, зокрема, нещодавнім накладенням великого штрафу на одного з великим телекомунікаційних операторів – TIM, за: «невідповідну агресивну маркетингову рекламу, збір персональних даних згоди та необґрунтований термін зберігання персональних даних» [48].

Варто зауважити, що Італія – країна, яка найпослідовніше і найшвидше внесла зміни в своє законодавство щодо імплементації положень GDPR змінивши Personal Data Protection Code (далі - "**PDPC**") [49]. На відміну від інших країн ЄС, Італія не приймала новий нормативно-правовий акт для приведення законодавства до стандартів GDPR, а внесла зміни у чинне законодавство уточнивши окремі аспекти правового регулювання, які були змінені GDPR. Зокрема, Декретом № 101 від 10 серпня 2018 року, яким було впроваджено положення GDPR в італійське законодавство, вносяться особливості щодо обробки чутливих категорій даних, обробки персональних даних судами, конфіденційності при електронній комунікації, встановлюються штрафи відповідно до штрафів, що передбачені у GDPR [50]. Крім того, Декрет також «встановлює принцип неможливості використання даних, які оброблялися з порушенням вимог законодавства» [50]

Особливістю, яка вирізняє Італійський PDPC, є його структура. PDPC побудований у формі кодексу, який містить окремі частини, щодо регулювання окремих сфер даних – судова сфера, діяльність поліції, державна безпека і оборона, освіта, охорона здоров'я та громадський сектор [51]. Водночас передбачено, що окремі сфери «можуть регулюватися підзаконними актами, які будуть видаватися Garante (*італійський наглядовий орган*)» [50].

Окремо в PDPC регламентовано і захист особистих даних померлих осіб. Зокрема, передбачається «що права, зазначені у статтях 15-22 GDPR, можуть здійснювати будь-хто, хто має в цьому певний інтерес, або виступає в ролі представника померлої особи, або через сімейні інтереси, якщо вони потребують захисту, якщо законом не передбачено інше»[52].

Варто також додати, що порушення обробки персональних даних за PDPC може мати наслідком притягнення осіб до кримінальної відповідальності, зокрема: «новими злочинами, запровадженими Декретом, є: незаконне передавання та розповсюдження персональних даних, коли обробка відбувається з метою отримання прибутку… отримання персональних даних шахрайським шляхом» [53].

Окремої уваги заслуговує італійський наглядовий орган – Garante per la protezione dei dati personali (далі - «**IDPA**», «**Garante**») [54], який «складається з Комісії та Бюро» [51]. Формування Комісії цього наглядового органу покладено на парламент Італії, а не на уряд (два представники призначаються Палатою депутатів, два інших – Сенатом [51]), що виокремлює Garante з виконавчої гілки влади Італії та робить його як можна менше залежним від уряду країни. Такий підхід найкраще демонструє вимоги GDPR щодо незалежності наглядових органів. Це так само, підтверджується італійськими юристами, які пишуть зокрема про те, що: «IDPA є незалежним адміністративним органом. Його незалежність зумовлена неупередженістю щодо публічної адміністрації та уряду (IDPA є не контролюється та не призначається урядом та є фінансово незалежним)» [55]

Бюро Garante, яке повинно мати як мінімум 162 посадові особи, покликане забезпечувати його діяльність і виконання поставлених завдань, в тому числі розгляд окремих кейсів[51]. Так само, до Бюро, за необхідності, може бути залучена обмежена кількість посадовців з інших органів державної влади [51].

Водночас, як і для працівників інших наглядових органів, для працівників Garante встановлені вимоги щодо незалежності та збереження конфіденційності при виконанні ними своїх обов’язків [51].

Повноваження Garante не відрізняються від інших наглядових органів і полягають у: «контролі за обробки персональних даних…; реагуванні на скарги суб’єктів даних; повідомленні про злочини…; притягненні до відповідальності контролерів та операторів даних; підготовці пропозицій уряду та парламенту Італії щодо необхідності прийняття змін у законодавство …» [49].

Варто також зауважити, що італійський наглядовий орган, затверджує та оновлює етичні правила що обробки персональних даних у певних сферах. Зокрема, на даний час існують етичні правила для сфер: журналістської діяльності, проведення розслідувань та захисту у суді, ділової інформації, статистичних та наукових досліджень та споживчого кредитування [49].

1.3.4 Угорщина

Угорщина є однією із найбільш активних країн щодо практичного застосування положень GDPR в Європі та впевнено лідирує щодо кількості кейсів в східній Європі [33]. Крім того, ця країна розташована близько країн Східного партнерства, що підвищує вагомість аналізу її підходів.

Основою угорського захисту персональних даних, як і для більшості інших країн ЄС, є окремий закон – CXII від 2011 року про свободу самовизначеності та свободу інформації [56]. Варто відзначити, що це перша з проаналізованих країн, яка поєднує захист персональних даних і право на свободу інформації в одному законі.

Варто відзначити й чітку розмежованість між сферами застосування цього та іншого законодавства щодо обробки даних. Вищезгаданий закон має таку ж сферу застосування, що і GDPR, а також застосовується до сфери обробки персональних даних у сфері національної безпеки та правоохоронної діяльності [57], в той час, як в інших галузях, як от медицина, трудова сфера, електронна комерція, фінансова сфера, маркетинг та електронні послуги, є окремі або додаткові нормативно-правові акти [56].

Важливо також зауважити, що національне законодавство Угорщини достатньо часто повторює GDPR, навіть, якщо в інших країн ці положення регулярно змінюються. Прикладом може бути вік з якої дитина може надавати згоду на обробку персональних даних. В Угорщині цей вік – 16 років [58]. Це єдина країна, з проаналізованих мною на цей час, яка не змінювала цей вік у порівнянні з GDPR.

Водночас угорський закон містить і незвичайні положення, як, наприклад, визначення строку зберігання даних, який встановлено на рівні строку позовної давності [58]. Крім того, за угорським законодавством є можливим розголошення персональних даних державними органами у суспільних інтересах [59].

Ситуація з можливим розголошенням персональних даних в Угорщині не так давно (весною 2020 року у розпал першої хвилі пандемії COVID-19), спричинила резонанс як в Угорщині, так і загалом в ЄС. Після введення в країні надзвичайного стану для боротьби з пандемією, уряд країни оголосив про: «Призупинення права на доступ до персональних даних та права на видалення персональних даних, а тим, хто подає скарги чи бажає скористатися правом на судовий захист, доведеться почекати поки уряд не проголосить припинення надзвичайного стану в країні» [60].

Хоча, GDPR і передбачає, можливість держави-члена ЄС відступати від положень Регламенту в деяких випадках, про що прямо зазначено у статті 23 GDPR [3], такі заходи викликали суперечності в угорському політикумі і така заява стала першою гучною заявою держави-члена ЄС, щодо відмови дотримуватися вимог GDPR. Звичайно, ця заява майже відразу отримала відповідь від EDPB, голова якої виразив своє глибоке занепокоєння такими заявами й відсутність підтримки таких заходів від EDPB [61]. Хоча подальшого розвитку чи інших санкцій зі сторони ЄС не було.

Наглядовий орган Угорщини – Nemzeti Ada tvedelmi es Informacioszabadsag Hatosag (далі – «**NAIH**») має надзвичайно широкі повноваження, як щодо проведення процедур перевірка та нагляду за збереження даних, сертифікації та затвердження корпоративних правил, так і щодо ініціювання кримінальних чи дисциплінарних проваджень [58].

NAIH є автономним органом згідно з угорським законом [57], водночас його керівник призначається президентом Угорщини на дев’ятирічний строк [57]. Варто також зазначити, що серед вимог до керівника – Президента NAIH, є вимога щодо наявності юридичної освіти [57], що не зустрічається в законодавстві інших країн. Крім того, Президент NAIH, згідно з параграфом 42 Закону, повинен «подавати декларацію про майновий стан … протягом тридцяти днів з момент =у призначення, а також кожного року до тридцять першого січня та після припинення повноважень» [57]. Такі вимоги передбачені безпосередньо

в законі, який прийнятий для захисту даних, вперше зустрічаються в ході мого аналізу.

З огляду на вищесказане, можна стверджувати, що угорське законодавство щодо захисту персональних даних має деякі особливості, які не є властивими навіть країнам західної Європи.

1.3.5 Німеччина

Німеччина займає одну з центральних позицій в ЄС. Особливо її роль зростає після виходу з Союзу Великої Британії. Крім того, Німеччина є однією з найбільш прогресивних країн у сфері захисту персональних даних, оскільки саме у Німеччині було прийнято перше законодавство в історії, яке стосувалося цієї сфери [62].

Так само і при імплементації GDPR в національне законодавство, Німеччина стала однією з перших країн, яка внесла зміни у своє законодавство. Bundesdatenschutzgesetz – німецький закон про захист персональних даних (далі – «**BDSG**») «був офіційно оприлюднений 5 червня 2017 року і набрав чинності разом з GDPR – 28 травня 2018» [63]. BDSG імплементує положення GDPR в німецьке законодавство та, водночас доповнює регулювання в окремих сферах – зайнятості та відеоспостереження [64]. В той же час не виникає питання про можливий конфлікт норм, оскільки: «положення BDSG не застосовуються, якщо є можливим застосування GDPR, оскільки його положення вважаються нормою вищою за ієрархією» [65].

Водночас окремі галузі законодавства Німеччини мають додаткове або окреме регулювання. Сюди можна віднести «сферу телекомунікації, електронних медіапослуг, охорони здоров'я» [64].

BDSG має окремі положення, які відрізняються чи доповнюють GDPR. Так зокрема, можна відзначити, що BDSG встановлює чіткий критерій для контролерів і операторів даних для призначення DPO – «якщо щонайменше 10 працівників компанії регулярно беруть участь в обробці даних» [66]

Крім того, BDSG вводить додаткові заходи юридичної відповідальності, які не передбачені GDPR. Зокрема, закон передбачає штрафи у розмірі 50 тис. євро за порушення положень виключно BDSG [67]. Крім того, німецький закон передбачає можливість відшкодування контролерами та операторами даних моральної шкоди завданої суб'єкту даних [67].

Водночас BDSG буде застосовуватися також до регулювання використання компаніями cookie-файлів, оскільки німецьке законодавство не передбачає окремого нормативного регулювання щодо використання цих засобів [65].

Також варто зауважити, що окремі закони про захист персональних даних діють у кожній окремі федеральній землі Німеччині і регулюють обробку даних в межах цих земель [68].

Неоднаково розподілено федеральне регулювання і за сферами обробки персональних даних. Так, BDSG містить окремі положення щодо регулювання працевлаштування та особливості обробки персональних даних що стосуються охорони здоров'я [69]. В той же час, окреме правове регулювання, як і в інших проаналізованих країнах ЄС, має сфера електронних та телекомунікаційних послуг, яка регулюється – TMG [68].

Як і нормативне регулювання, кожна з федеральних земель Німеччини має окремий власний наглядовий орган [70]. Але, оскільки GDRP передбачає, що при створенні багатьох наглядових органів у державі, представляти її в ЄС, має лише один наглядовий орган [3], таким наглядовим органом у Німеччині виступає – Der Bundesbeauftragte fur Datenschutz und die informationsfreiheit (далі – «**BDI**»).

BDI призначається на посаду німецьким парламентом за пропозицією уряду країни [69]. На відміну, від Угорщини, де є прямі вимоги про вищу юридичну освіту кандидатів на посаду керівника наглядового органу, німецьке законодавство передбачає виключно вимоги щодо наявності «кваліфікації, досвіду та навичок, зокрема у галузі захисту персональних даних… Зокрема, … повинен знати законодавство про захист персональних даних, отриманні протягом здійснення професійної діяльності»[69].

Досить схожим на призначення BDI, є призначення керівників наглядових органів окремих федеральних земель. Вони призначаються місцевими Бундесратами та, крім того, що очолюють наглядові органи в окремих землях Німеччини, водночас стають заступниками BDI [71]. Таким чином, досягається баланс між автономністю окремих земель у складі Німеччини та вимогами GDPR щодо механізму послідовності.

Повноваження наглядового органу Німеччини не відрізняються суттєвим чином від аналогічних повноважень наглядових органів інших країн і вміщують в себе моніторинг дотримання законодавство, надання консультацій німецькому парламенту та уряду, розгляд скарг та проведення розслідувань і т.д. [71].

***

Питома вага положень GDPR, які дозволяють дискрецію державам-членам ЄС є досить високою, що свідчить про можливість держав-членів ЄС вирішувати окремі питання на рівні національного законодавства.

Так само GDPR передбачає достатньо широкі повноваження для наглядових органів окремих країн, які фактично повинні бути забезпеченими всіма ресурсами зі сторони держави-члена ЄС та водночас залишатися повністю незалежними, як від внутрішнього, так і від зовнішнього впливу. В цьому контексті, найбільш ефективний механізм забезпечення незалежності наглядового органу передбачено законодавством Італії, де повноваження з формування наглядового органу покладено на парламент, а не на уряд країни, який, в свою чергу, забезпечує наглядовий орган ресурсами.

Окремі аспекти територіальної дії GDPR дозволяють говорити про екстериторіальність його дії. Зокрема, цей аналіз обгрунтований також наявністю практики притягнення наглядовими органами ЄС до відповідальності контролерів та операторів, до яких GDPR застосовується виключно за критерієм «цільового спрямування».

Важливим є наявність у GDPR окремих критеріїв, які повинні впливати на розміри відповідальності контролерів. Вони активно використовуються

окремими наглядовими органами та сприяють більш пропорційному визначенню обсягу відповідальності.

Структура наглядових органів на наднаціональному рівні в ЄС характеризується чітким розподілом повноважень і завдань між такими органами. Попри певну ієрархічну побудову системи органів та підзвітність EDPB іншим органам Європейського Союзу, все ж можна відзначити наявність достатніх повноважень в EPDB, щоб не залишатися виключно консультативним органом ЄС, а тлумачити GDPR та вирішувати певні суперечності, що виникають між наглядовими органами різних країн, що робить EDPB центром формування практики застосування GDPR.

Водночас в результаті аналізу національного законодавства, варто зауважити, що держави-члени досить часто користуються дискреційними можливостями щодо врегулювання окремих правовідносин в національному законодавстві. Проте, більша частина країн, які були проаналізовані, прагнуть, з метою встановлення однакового правозастосування, включити у сферу дії свого законодавства, яке приведено стандартів GDPR, як можна більше різних сфер, де здійснюється обробка персональних даних.

Крім того, держави-члени достатньо по-різному підходять до формування законодавства в сфері захисту персональних даних. Вирізняється, італійське законодавство, де діє окремий кодифікований нормативно правовий акт спрямований на регулювання сфери захисту персональних даних. Водночас для більшості країн, характерним є намагання виділити окремі сфери, такі як, цифровий маркетинг та національна безпека, і врегулювати обробку персональних даних в цих сферах окремими нормативно-правовими актами.

В контексті функціонування наглядових органів вагомим є існування чіткої тенденції щодо формування одного потужного наглядового органу з можливістю створення окремих підрозділів. Це, своєю чергою, не розмиває повноваження наглядових органів та запобігає можливим суперечностям у їх роботі.

За результатами аналізу національного законодавства, варто зазначити, що окремі держави-члени ЄС надають додаткової уваги відповідальності операторів та контролерів даних перед суб'єктами даних. Зокрема, німецьке законодавство передбачає відшкодування моральної шкоди за заподіяну шкоду.

РОЗДІЛ 2. Сучасні виклики у сфері захисту персональних даних та правові шляхи їх розв'язання

2.1 Аналіз останніх справ щодо найчастіших порушень GDPR в країнах ЄС

2.1.1 Порушення принципів обробки персональних даних

Важливою частиною моєї роботи, я вважаю аналіз особливостей правозастосування норм і положень GDPR. Оскільки, Регламент вносить багато змін у сферу захисту персональних даних, вводячи нові та розширюючи вже існуючі інститути, на мою думку, правозастосування цих норм повинно займати центральне місце при дослідженні GDPR.

Водночас оскільки Регламент діє вже протягом майже двох років, я переконаний, що можна говорити про цілком вибудовану практику наглядових органів держав-членів ЄС у тлумаченні та застосуванні положень GDPR, а не про окремі рішення в окремих кейсах.

Як вже зазначалося у першому розділі цієї роботи, принципи закріплені у статті 5 GDPR стають основою і фундаментом для більшості інших положень GDPR. Крім того, оскільки вони уособлюють мету прийняття GDPR та сформульовані достатньо лаконічно, не виникало сумніву, щодо того, що наглядові органи різних країн будуть будувати свою аргументацію щодо порушення контролерами та операторами якраз на цих положеннях GDPR.

За базою даних компанії CMS, більш ніж кожен другий штраф – 328 із 548 кейсів GDPR (на момент написання цієї частини роботи), що становить майже 60% всіх кейсів, містять порушення статті 5 про принципи обробки персональних даних GDPR [23]. Так само, застосування статті 5 є найбільш поширених серед країн механізми захисту, яких було проаналізовано мною у попередньому розділі. У Великої Британії це 2 з 4 кейсів, в Іспанії – 120 із 183, в Італії – 39 із 44. [23].

Гучні кейси, що є пов’язані із застосування принципів GDPR, має кожен наглядовий орган держав-членів ЄС. Водночас найбільш відомими є кейси ICO щодо порушення Ticketmaster [72] і British Airways [73].

Обидва кейси стосуються несанкціонованого доступу до персональних даних суб’єктів даних, що користувалися послугами компаній, третіми особами. Зокрема, йдеться про інформацію щодо банківських рахунків, які надавалися компаніям її клієнтами. Варто також зауважити, що обидва порушення сталися приблизно в один і той же час: Ticketmaster – весна і початок літа 2018 року [72] (порушення почалося ще до вступу в дію GDPR, але ICO розглядав порушення лише щодо травня-червня 2018 року) [72], а British Airways – літо 2018 року [73].

Tickemarket при наданні послуг використовував чат-бота іншої компанії Inbenta для спілкування зі своїми клієнтами. Код вказаного чат-бота мав недолік, який дозволив третім особам отримати через бота кілька тисяч даних про банківські картки (йдеться про номери банківських карток, строки їх дії та CVV) [72]

Це стало основою аргументації Ticketmarket щодо доведення відсутності порушення зі сторони компанії. Згідно з пунктом 5.11 рішення ICO у цій справі, звинувачена у порушенні статті 5 і 32 GDPR Ticketmarket мала чотири контраргументи проти звинувачень у їх сторону: «Порушення спричинила недбалість зі сторони Inbenta; порушення було неможливо передбачити; Ticketmarket вживали належних заходів для забезпечення безпеки даних; висновки ICO є помилковими» [72].

Хоча такі аргументи могли би бути дієвими, особливо, з огляду на умови договорів між компаніями, які мали положення про збереження даних на серверах Inbenta, ICO, як це зрозуміло з пункту 6.3 рішення, проте ICO зайняв тут чітку позицію, що в контексті положень статті 5 GDPR: «Контролер даних, у даному випадку Ticketmarket, є відповідальним за це і повинен бути в змозі це продемонструвати (йдеться про захист від несанкціонованого втручання)» [72].

Натомість British Airways, у своєму кейсі, не мала таких аргументів. Порушення полягало в отриманні доступу до даних про банківські рахунки

третіми особами, що призвело до можливості третіх осіб «у період з 14 по 25 серпня 2018 року … переспрямовувати дані про банківські рахунки користувачів на інший вебсайт: «BAways.com». Порушники були власниками і адміністраторами сайту «BAways.com» [73].

У своєму прес-релізі щодо обставин цього кейсу, ICO заявив, що: «існували численні заходи, які BA міг здійснити для пом'якшення або запобігання ризику доступу сторонніх осіб до мережі BA. Серед них:

Обмеження доступу до програм, даних та інших інструментів тільки тими, які дійсно необхідні для використання користувачем;

Проведення ретельної перевірки у формі імітації кібератак

Захист облікових записів співробітників та інших компаній за допомогою багатофакторної автентифікації» [74].

Жоден з таких, чи подібних заходів, не вживалися British Airways. Водночас варто відзначити, що в обох кейсах ICO звертав увагу на діяльність контролерів даних щодо запобігання таких ситуацій в подальшому.

Ірландські наглядові органи, так само. звертаються до статті 5 GDPR у випадках несанкціонованого доступу до персональних даних. Так, у кейсах щодо порушення статті 5 і 32 GDPR, які були здійсненні коледжем дублінського університету, було встановлено порушення, яке полягало у тому, що: «дані про вхід до деяких облікових записів службовців університету було розміщено у вільному доступі» [75]. Крім того, DPC також звинувачував коледж у «надмірних строках обробки персональних даних» [76] та «пізньому повідомленні про факт порушенні» [76].

Варто також зауважити, що цей кейс стосується не приватної компанії, а державного навчального закладу, що свідчить про застосовність положення щодо поширення дії GDPR на державні органи.

Так само, достатньо частим є застосування статті 5 GDPR у сукупності зі статтею 6, що стосується законності обробки персональних даних. Прикладом, такого кейсу, може стати випадок порушення, зафіксований болгарським наглядовим органом – Комисия а защита на личните данни (далі – «**КЗЛД**»).

Справа стосувалася транскордонної передачі даних, яка відбувалася між Міністерством внутрішніх справ Болгарії та урядом Того щодо громадянина Фінляндії, яким мав однакове ім'я та прізвище з особою, яка розшукувалася урядом Того через Інтерпол [77]. Оскільки замість отримання даних про особу з Того, Міністерство внутрішніх справ Болгарії відправило дані затриманої особи-суб'єкта даних, цей суб'єкт звернувся до КЗЛД зі скаргою на порушення порядку обробки персональних даних та незаконну передачу даних у Того. [77]

Варто зауважити, що це перший з розглянутих мною кейсів, які були ініційовані індивідуально, однією особою, і порушення спричиняло шкоду виключно одній особі. За результатами розгляду скарги було визнано, що «Міністерство внутрішніх справ обробляло персональні дані незаконно, без гарантування їхньої безпеки, всупереч принципам обробки персональних даних, … що полягало у передачі персональних даних Того без належних правових підстав» [77].

Застосування принципів GDPR і до транскордонної передачі даних, на прикладі цього кейсу, ще раз підкреслює загальність цих принципів у сфері персональних даних сучасного ЄС.

Аналізуючи кейси щодо принципів обробки даних, варто також згадати про велику групу компаній, яка має найбільше порушень у цій галузі. Група компаній Vodafone, на момент написання роботи, має вже 38 справ про порушення положень GDPR у трьох різних країнах ЄС – Італії, Румунії та, найбільше, Іспанії [23].

Найбільший з цим кейсів за сумою штрафу є єдиний італійський кейс, який пов'язаний з маркетинговою послугою Компанії. Garante розглядала цю справу після «численних скарг користувачів щодо телефонних дзвінків від компанії з метою маркетингу своїх послуг» [78]. Наглядовий орган Італії знайшов численні порушення щодо використання незаконних баз телефонних номерів, підроблених телефонів і так далі, що свідчили про «абсолютне нехтування італійським законодавством щодо захисту персональних даних зі сторони компанії» [78].

Вищезгадані кейси дозволяють з впевненістю сказати, що принципи обробки персональних даних застосовуються наглядовими органами у будь-яких ситуації, більше того, аналіз дій контролерів та операторів даних починається з аналізу ситуації з точки зору дотримання принципів. Крім того, можна стверджувати, що принципи застосовуються до ситуацій незалежно від умов і критеріїв, які містяться в GDPR – територіальність, транскордонна обробка даних і т.д.

Крім цього, варто зауважити, що на прикладі справи Ticketmarket, можна чітко переконатися, що при порушеннях GDPR компанія не матиме можливість перекласти відповідальність за порушення на своїх контрагентів, навіть, якщо вони неналежним чином виконали свої зобов'язання перед компанією.

2.1.2 Законність та умови надання згоди на обробку персональних даних

Законність обробки персональних даних та правильність надання згоди суб'єктами персональних даних для дотримання вимог GDPR набули великого значення, з огляду на нововведення передбачені Регламентом.

Досить часто, стаття 6 і 7 GDPR застосовуються контролюючими органами різних країн в поєднанні зі статтею 5, принципами обробки персональних даних. Водночас я вважаю, що ця категорія справ має окрему специфіку і є більш вузькою, ніж сфера застосування статті 5.

Аналіз кейсів по цій тематиці, на мій погляд, потрібно почати з кейса, в рамках якого було накладено перший штраф за порушення GDPR і який водночас є найбільш узагальненим прикладом порушення вищезгаданих норм. Ірландський наглядовий орган, DPC, визнав порушення у діях державного агентства у справах сім'ї – Tusla, яке неправомірно поширювало персональні дані.

Порушення полягали у тому, що Tusla розкривала дані про осіб, які зверталися до неї, та інформацію про їх місцезнаходження третім особам,

порушуючи при цьому в тому числі та таємницю усиновлення. Зокрема, DPC розглядалося три конкретних випадки: «розкриття зловмиснику інформації про контакти та місцезнаходження матері і дитини; розкриття бабусі і дідові дитини інформацію контакти, місцезнаходження і шкільні дані дитини, яка знаходилася у прийомні сім'ї; розкриття інформації про місцезнаходження дитини у прийомні сім'ї, ув'язненому батькові» [79].

Tusla навіть не намагалася оскаржити таке рішення, оскільки обставини справи свідчили, що агентство не намагалося отримати дозвіл від суб'єктів даних на розкриття такої інформації. Більше того, агентство навіть не повідомило про витік такої інформації [80]. Інформація безконтрольно передавалася третім особам, які зверталися до організації.

Так само промовисто окреслює проблеми передачі даних кейс тенісної асоціації в Нідерландах. У 2020 році, асоціація була оштрафована за порушення кількох статей GDPR при поширенні персональних даних спонсорам асоціації.

Наглядовий орган Нідерландів з'ясував, що «спонсори зверталися до деяких учасників асоціації поштою або телефонували їм у маркетингових цілях» [81].

Варто зауважити, що нідерландський наглядовий орган в межах цього кейсу розглядав дві окремі ситуації щодо: «Обробки персональних даних членів асоціації, які вступили до неї до 2007 року та після 2007 року» [82]. Це пояснюється тим, що 2007 року, асоціація декларувала однією з цілей розвиток маркетингової діяльності асоціації в рамках, якої міг здійснюватися обмін інформацією [82].

Варто зауважити, що в обох випадках було знайдено порушення. І якщо, перша ситуація, щодо даних зібраних у 2007 році була очевидним порушення вимог GDPR щодо обробки персональних даних без законної мети, то другий випадок не був настільки однозначний.

Складність в такому випадку полягала у тому, що мета була задекларована асоціацією тенісу. Відповідно, персональні дані збиралися із законною метою. Саме тут наглядовий орган Нідерландів використовував положення статті 6

GDPR і обґрунтував порушення зі сторони контролера тим, що: «Асоціація не мала правової основи для обробки, оскільки, вона не отримувала згоду суб’єктів даних і відповідно, не може покладатися на законність підстав» [82].

З цього, на мою думку, можна зробити висновок про те, що незалежно від того чи задекларував контролер чи оператор цілі використання даних, важливим, в аспекті законності обробки, залишається конкретна можливість контролера та оператора довести, що кожен суб’єкт даних усвідомлював цілі з якими збиралися такі дані і надавав свою згоду на таку обробку.

Подібний кейс, також був у Іспанії, де AEPD наклав штраф на футбольний клуб хіхонський Спортинг за «за незаконний збір суб'єктів даних з метою надсилання повідомлень з цілями маркетингу» [83]. Відповідно, проблеми безконтрольного використання персональних даних для цілей маркетингових досліджень зустрічаються в різних державах-членах ЄС.

Достатньо актуальним в умовах сучасного розвитку технологій є кейс щодо порушення GDPR іспанською футбольною лігою – La Liga. Можна погодитися з думкою, що: «У цьому рішенні було відображено ряд ключових питань правової парадигми сьогодення у сфері захисту персональних даних, зокрема, деякі питання, що є важливими для використання мобільних додатків» [84].

Цей кейс не пов’язаний з маркетинговою діяльністю і передачею персональних даних третім особам. Водночас він є демонструє складність у трактуванні різноманітних ситуацій, що пов’язані з застосуванням сучасних технологій.

La Liga, які і велика кількість інших спортивних організацій світу, має власний додаток для смартфонів. Крім того, як і більшість спортивних організацій у світі, La Liga зацікавлена у боротьбі з таким явищем, як піратство.

Для боротьби з цим явищем, у рамках офіційного додатка діяв спеціальний функціонал: «захищай свою команду», який повинен був допомагати слідкувати за можливими порушеннями прав інтелектуальної

власності в барах та ресторанах» [84]. Тобто, такі дані використовувалися La Liga для контролю неліцензованої трансляції поєдинків турніру.

При встановленні цього додатку, як і будь-якого іншого, додаток просив дозвіл у користувача на отримання доступу до численної кількості функцій смартфонів, зокрема, і до мікрофона та даних геолокації. Водночас «Додаток не повідомляв користувачів про те, чому такі дані збираються і, відповідно, користувачі, взагалі не мали інформації про те, чому збираються аудіо та дані геолокації» [85]. Проблема також полягала у тому, що додаток робив записи та визначав місцезнаходження осіб, навіть «якщо додаток активно не використовувався» [84]. В подальшому програми порівнювали зроблений запис із записом матчу і виявляли порушення прав інтелектуальної власності.

AEPD розглядав це як порушення GDPR щодо незаконності обробки таких даних. Хоча La Liga оскаржувала рішення, її аргументи не знайшли підтримки. Зокрема, футбольна асоціація висловлювалася про те, що: «Програма насправді не отримує доступу до зібраних аудіозаписів, оскільки вони автоматично перетворюються у двійковий код, який в подальшому використовується лише для перевірки відповідності контрольному коду» [85].

Як я розумію, La Liga мала на меті обгрунтувати те, що такі записи не є персональними даними, оскільки не дають змоги ідентифікувати будь-якого суб’єкта даних. Але цей аргументи було відкинуто, оскільки «форма, в якій було зібрано персональні дані немає значення» [85].

Так само, було відкинуто аргумент La Liga щодо того, що суб’єкти даних могли використовувати додаток, навіть, у випадках, коли вони не давали дозвіл на збирання вищезгаданих даних [86]. Хоча він і був використаний La Liga для її захисту, такий аргумент, на мій погляд, навпаки діє на шкоду позиції футбольної асоціації, оскільки залишає без обгрунтування питання щодо того, навіщо в такому випадку La Liga запитувала такі дозволи загалом.

Останнє, що хотів би додати щодо цього кейсу, це позиція AEPD щодо того, що поінформованість користувачів: «Повинна бути посиленою при цьому типі обробки персональних даних за допомогою символів, що повинні з'являтися

на екрані, коли активується функція GPS або мікрофона, або навіть за допомогою «push» чи «pull» сповіщень, які надають користувачам інформацію в режимі реального часу» [85].

Тобто, іспанський наглядовий орган не відкидає можливості застосування таких технологій загалом, лише обґрунтовує необхідність підвищеної інформатизації для користувачів щодо такого функціоналу.

2.1.3 Обробка спеціальних категорій персональних даних

GDPR передбачає специфічні умови для обробки так званих «sensitive data», специфічних категорій даних. Як, я розумію, це пояснюється природою таких даних, оскільки до них GDPR включає дані про: «расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і опрацювання генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації» [3].

Тобто, це досить широкий перелік даних, які, скоріше за все, можна поєднати тим фактом, що суб'єкти даних зазвичай надають перевагу залишенню цих даних у таємниці. Таким чином зрозуміло, що особливість тут полягає у специфічному предметі таких справ – безпосередній специфічності таких даних. З огляду на це, можна назвати ще одну узагальнюючу рису цих справ – здебільшого контролером таких даних виступають медичні заклади або заклади освіти. Також не виключенням є органи державної влади.

Перший кейс, який я хочу описати, специфічний тим, що йдеться не про електронні персональні дані, як у кейсах, що згадувалися у попередніх підрозділах. Натомість в даному кейсі, порушення передбачало недбале зберігання персональних даних, які зафіксовані на паперових носіях.

Справа стосується штрафу накладеного ICO на одну з аптек Лондона. Порушення полягало у тому, що «Аптека «Doorstep Dispensaree Ltd» залишила

близько 500 000 документів у незамкнених контейнерах, сумках та коробках у замкненому дворику в задній частині свого приміщення» [87]. Оскільки мова йде про медичний заклад, зрозумілим є те, що дані які зберігала аптека про свої клієнтів можна відносити до чутливих даних, оскільки ця інформація стосується стану здоров'я таких осіб.

Зокрема, у своєму висновку ICO пише про те, що в документах містилася інформація: «Ім'я, адреса, дата народження, NHS номер, медична інформація та приписи лікаря» [88].

Оскільки аптека не вживала жодних заходів для збереження конфіденційності цих даних ICO вважав, що компанія порушила цілий ряд статей GDPR, які стосуються вимог щодо обробки персональних даних. Зокрема, красномовною є цитати одного з керівників ICO, Стіва Екерслі, яка наведена в прес-релізі ICO щодо цього випадку: «Недбалий спосіб, яким Doorstep Dispensaree зберігав чутливі категорії даних, не захистивши від випадкових пошкоджень або їх втрати. Це не відповідає тому, що очікує закон, і тому, що очікують люди» [89].

Водночас незавершеним для мене у цій справі залишається одне питання. Рішення ICO ніяким чином не стосується обґрунтованості строків зберігання персональних даних. Незрозуміло залишається, яким саме чином аптека змогла обґрунтувати необхідність зберігання такої інформація, як, наприклад, приписи лікаря. А оскільки, якщо слідувати умовам, деякі документи могли залишатися в аптеці на довгий час [90], виникає питання чому не було окремо розгляду щодо підстав зберігання таких даних.

Інший кейс щодо обробки персональних даних буде стосуватися застосування новітніх технологій розпізнавання обличчя. Такі технології були використані Secondary Education Board (далі – «**EDU**») у Швеції з метою моніторинг відвідуваністю учнями занять. Зокрема, EDU пояснювала, що: «Реєстрація відвідуваності звичним способом займає десять хвилин уроку. А технологія розпізнавання обличчя дозволить зекономити 17 280 годин на рік у кожній школі» [91].

Звісно використання технології розпізнавання облич буде означати обробку персональних даних, оскільки в такому випадку відбувається обробка біометричних даних. Водночас шведський наглядовий орган наголошує на тому, що в конкретних умовах: «Відносини між EDU та студентам, зазвичай, характеризуються значним дисбалансом і моніторинг поведінки відвідуваності є одностороннім заходом контролю там, де існує нерівність» [91].

Базуючись на цьому, шведський наглядовий орган дійшов висновку, що застосування передбаченої частиною 2 статті 9 GDPR можливості обробки чутливих персональних даних є неможливим в такому випадку, навіть не дивлячись на те, що була отримана згода на таку обробку.

Як я вже писав, порушення вимог до обробки персональних даних закладами освіти є досить частим явищем і характеризується достатньо недбалим ставлення до зібраних персональних даних. Так, наприклад, у вже згаданій Швеції, дослідницька група університету Умео отримувала від поліції і зберігала інформацію про злочини проти статевої свободи без жодного шифрування [92]. За словами однієї з працівниць шведського наглядового органу: «Хмарний сервіс та його використання університетом, не забезпечувало достатньо захисту для цього типу персональних даних» [92]. Загалом, на мою думку, що зберігання будь-яких персональних даних з використанням хмарних технологій, незалежно від категорії, не може вважатися достатньо захищеним, оскільки слабко зменшує ризик витоку персональних даних і отримання доступу щодо них третіми особами.

Водночас не тільки заклади освіти нехтують безпекою даних при використанні новітніх технологій.

Так, наприклад, португальська міська лікарня була оштрафована з порушення GDPR при обробці персональних даних їх пацієнтів. Зокрема суть порушення полягала у тому, що: «Персонал лікарні, психологи, дієтологи та інші фахівців мали доступ до даних пацієнтів через неправдиві профілі. В електронній системі лікарні було зареєстровано 985 лікарів, хоча насправді працювало лише 296. Більше того, лікарі мали необмежений доступ до всіх файлів пацієнтів,

незалежно від спеціальності» [93]. Такий підхід суперечить не тільки статті 9 GDPR, але і прямо суперечить відразу кільком іншим положення GDPR щодо обробки звичайних категорій персональних даних.

Водночас не спрацював основний аргумент лікарні, яка пояснювала таку ситуацію тим, що: «використовує інформаційну систему, що надається державним лікарням Міністерством охорони здоров'я Португалії» [94]. Відповідно, з цього можна зробити висновок, що відповідальність за GDPR носить чітко індивідуалізований характер і контролерам персональних даних, які є державними установами не вдасться уникнути штрафів за порушення вимог через перекладення відповідальності на інші державні органи.

2.1.4 Повідомлення суб'єктам даних інформації, що стосується обробки їх даних

Як і попередні аналізовані мною категорії справ щодо порушень положень GDPR, справи, пов'язані з повідомленням суб'єктів даних належить до найбільш поширених. Водночас варто зазначити, що порушення статей 13 та 14 GDPR досить часто супроводжується порушенням інших статей, як, наприклад, 5, 6 чи 12 GDPR.

Це зрозуміло, з огляду на положення самих статей, які спрямовані на встановлення вимог щодо обсягів інформації, які має отримати суб'єкт даних за умови як контролер отримує від нього (стаття 13) чи від іншого контролера (стаття 14) персональні дані для подальшої обробки. Зокрема, йдеться про контактні дані контролерів та Data protection officer, цілей опрацювання даних, інших одержувачів. [3]

Перший кейс в рамках цього аналізу буде так само поєднанням порушень згідно зі статтями 6 і 13 та 14 GDPR. Справа стосувалася одного з іспанських банків, який змінив політику опрацювання даних у 2018 році [95]. Зокрема, розслідування було ініційоване зверненням особи, яка вважала непропорційною дії CaixaBank щодо: «Розгляду можливості передачі персональних даних своїх

клієнтів всім компаніям банківської групи і що для припинення обробки даних кожною з цих компаній групи, суб'єкту даних необхідно звернутися до однієї з цих компаній» [95].

AEPD наклав на банк санкції одразу за два порушення – 2 млн Євро за порушення статті 14 і 4 млн Євро за порушення статті 6 [95]. Такий чіткий розподіл суми штрафу за порушення окремих статей рідко зустрічається серед рішень наглядових органів різних держав-членів ЄС.

Специфіка порушення за статтями 13 і 14 GDPR полягала у тому, що: «Інформація, що надається CaixaBank в різних документах і каналах, не є однорідною, в Privacy Policy неточна термінологія, а інформація про категорії персональних даних, що обробляються, профілі користувачів та їх конкретне використання, а також здійснення прав та періоди зберігання даних була недостатньою» [96].

Таким чином, з цього слідує, що в рамках статті 13 і 14 наглядові органи розглядають широкий спектр проблем щодо надання інформації суб'єктам даних та правильності складання політики обробки персональних даних.

Інший кейс стосується так само Іспанії, зокрема компанії Miraclia та мобільного додатку «Juasapp», який дозволяє користувачам розігрувати один одного змінюючи голос. [97].

Розгляд справи було ініційовано кількома скарга користувачів, які просили Miraclia видалити їх персональні дані, на, що компанія давала відповідь, що немає змоги цього зробити, оскільки не обробляє персональні дані та запис розмови , а лише керує роботою додатку. [97] Крім того, у рішенні по справі описується цей процес: «Користувач завантажує додаток і приймає його умови. Після цього створюється профіль користувача для використання послуги передачі голосу через IP пристроя і йому надається окремий номер, який використовується додаток… Щоб скористатися додатком, потрібно обрати жарт із пропонованого каталогу і ввести номер телефону одержувача жарту та обрати дату та час дзвінку» [97]. Майже відразу стає зрозумілим, що процедура достатньо складна і не буде зрозумілою для кожної особи.

Водночас компанія наполягала, що такі жартівливо записані розмови можуть бути поширюватися лише особами, яка зробила розіграш, позиціонуючи це як особливість додатку. [97]

За результатом розгляду цієї скарги AEPD притягнув до відповідальності Miraclia, водночас зазначивши, що в конкретних умовах є: «Важливим, що суб'єкти даних пропонував можливість заперечувати та видаляти дані» [97]. Саме це, а також відносно невелика кількість заяв від суб'єктів даних, вплинуло на остаточне покарання.

Ще одним, на мій погляд, найбільш узагальненим прикладом порушення статті 13 GDPR можна вважати справу щодо притягнення до відповідальності французької компанії Spartoo.

Як і попередні кейси, це було комплексне порушення положень GDPR, яке полягає у порушенні статей 5, 13, 32 GDPR. Зокрема суть справи полягала у тому, що: «Розслідування CNIL було зосереджено, зокрема, на файлах клієнтів та потенційних клієнтів Spartoo, а також на записі телефонних розмов між клієнтами та працівниками, які працюють у відділі обслуговування клієнтів» [98].

Водночас, що не зовсім своєрідно для інших кейсів, в такому випадку дотримання положень GDPR розглядалося французьким наглядовим органом як щодо клієнтів, так і щодо працівників компанії. Зокрема, порушення статті 13, крім недостатньої точності та недоліках у політиці обробки даних, були також обґрунтовані тим, що: «Працівники не були проінформовані про мету обробки персональних даних, правову основну обробки, одержувачів даних, термін зберігання даних та їх прав» [98].

Таким чином, при записі дзвінків жоден зі співрозмовників не був належним чином проінформований щодо деталей обробки даних.

Надзвичайно цікавим, якщо продовжувати лінію новітніх технологій, є також кейс про порушення GDPR іспанською компанією Grow Beats SL. Справа стосувалася, якраз застосування достатньо новітніх засобів накопичення і обробки персональних даних – файлів cookie.

Зокрема, компанія була на своєму сайті: «Посилалася у своїй Privacy Policy на попередній Закон про захист персональних даних, який не був адаптований до GDPR та не надавала користувачеві доступ до інформації, яка викладена в ньому на момент збору його персональних даних» [99].

Досить неочікуваним було таке порушення, оскільки компанії займається електронною комерцією і повинна достатнім чином слідкувати за своїми інформаційними ресурсами. Водночас застосування cookie-файлів без достатньої обґрунтованості було досить очевидним, що це спровокує перевірку від наглядових органів і застосування санкцій до компанії.

2.1.5 Дотримання безпеки при обробці персональних даних

Остання категорія справ, які будуть аналізуватися мною, стосується сфери забезпечення безпеки даних та запобігання можливому доступу до них зі сторони третіх осіб.

Як вже зазначалося у попередніх частинах моєї роботи, GDPR покладає на контролерів зобов'язання щодо забезпечення схоронності даних. І хоча формулювання в самому GDPR чітко передбачають, що «Контролер і оператор повинні вжити необхідних технічних і організаційних заходів для забезпечення рівня безпеки відповідно до ризику» [3], після чого йде перелік заходів, які варто вживати контролерам для збереження даних, все ж межі між належним та неналежним забезпеченням безпеки даних є недостатньо чіткими. На мій погляд, в контексті цієї статті, контролерам та операторам даних при витоку персональних даних досить складно, якщо взагалі не неможливо, довести, що дані були захищені належним чином. Це з моєї точки зору, не є коректним і ставить контролерів та операторів у незручне становище.

Водночас ймовірною є можливість напрацювання таких рамок у практиці діяльності наглядових органів та правозастосуванні норм GDPR.

Однією з найбільш відомих справ, пов'язаних із захистом даних, є справа щодо порушень вимог GDPR з боку Marriot International Inc у Сполученому

Королівстві. Насправді кейс стосується іншої мережі готелів – Starwood, проте на час проведення розслідування, вказана мережа була придбана готельним гігантом. [100]

Особливістю кейсу є також те, що в такому випадку розглядається триваюче порушення. Точніше кажучи, витік даних почався задовго до прийняття та набуття чинності GDPR – у 2014 році, коли відбувалася хакерська атака на інформаційну систему Starwood. Доступ отриманий хакерами дозволяв їм протягом довго часу безперешкодно отримувати персональні дані клієнтів готелю, оскільки шкідливі програми у своїй мережі контролер виявив лише 2018 року. [101]

Деталі кібератаки описані у прес-релізі ICO, де зазначено: «Зловмисник встановив частину коду на обладнання в мережі Starwood, який давав можливість віддаленого доступу та редагування даних, які містилися в мережі» [101].

На свій захист Marriot висунув цілий ряд аргументів, зокрема, щодо відсутності послідовності в заявлених звинуваченнях, безпідставності застосування GDPR та недоліки у визначеності у правилах, які застосовуються в такому випадку до нього [100], якими прагнув аргументувати свою непричетністю і невинуватість до витоку даних, який стався.

Водночас ICO знайшов порушення у діях Marriot, проте тільки щодо статті 32, хоча саме розслідування відбувалося як щодо порушення статті 32, так і щодо порушення статті 5 GDPR [100]. Водночас варто зауважити, що в даній справі ICO виступав, як LSA, оскільки фактично витік даних стосувався понад 339 млн осіб. Цей факт масштабності витоку даних, також враховувався ICO при обранні розміру штрафу для компанії [100].

Цей кейс демонструє достатньо суворий підхід наглядових органів до порушення, що стосуються вже наявного факту витоку персональних даних за GDPR. Подібний підхід ICO демонстрував і в інших своїх рішення, зокрема щодо British Airways та Ticketmarket, про які я писав у попередніх підрозділах.

Такої ж послідовності дотримується і наглядовим органом Ірландії, який притягнув до відповідальності за порушення статей 5 і 32 GDPR Дублінський

коледж з якого відбувся витік дані, який дозволив отримати доступ до службових профілів користувачів, який я теж описував вище [76].

Варто відзначити, що деякі компанія, які належать до однієї групи компаній і водночас є контролерами чи операторами даних, за відносно короткий час дії положень GDPR, вже встигли отримати по кілька штрафів від наглядових органів власних країн щодо порушення статті 32 GDPR. Так, прикладом може слугувати шведська компанія Aleris, яка спеціалізується на наданні медичних послуг. Дві компаній групи – Aleris Sjukvard AB [102] та Aleris Narsjukvar AB [103] були оштрафовані за порушення правил забезпечення безпеки даних.

Як і в першому випадку щодо компанії Aleris Sjukvard [102], так і в другому кейсі компанії Aleris Narsjukvard [103], занепокоєння наглядового органу викликали питання щодо безпечності електронної системи, яку використовувала компанія та її належного тестування.

Іншим прикладом подібної ситуації може стати група компаній Vodafone, які отримали кілька штрафів за порушення статті 32 GDPR в Іспанії. Їх причини - порушення положень статті 32 в усіх кейсах Vodafone схожа. Узагальнюючи, можна стверджувати, що порушення виникало через отримання клієнтами компанії персональних даних інших клієнтів [23].

Так само цікавим в контексті забезпечення належних механізмів захисту персональних даних можна вважати кейс німецької компанії 1&1 Telecom GmbH. Справа розглядалася BFDI у 2019 році і її суть полягала у тому, що: «Абонент мав можливість отримати доступ до детальної інформації щодо користувачів, назвавши лише ім’я та дату народження певного абонента» [104].

Очевидно, що ця ситуація мала викликати підозри щодо її відповідності вимогам статті 32 GDPR, оскільки за таких умов достатньо складно однозначно сказати, яким саме чином проводиться верифікація особи, яка отримує доступ до інформації. Позиція BFDI якраз і полягала у тому, що: «Ця процедура ідентифікації порушує статтю 32 GDPR, яка зобов’язує компанії вживати відповідних технічних та організаційних заходів для систематичного захисту персональних даних» [105]

Останній аспект, який би хотілося згадати в контексті забезпечення безпеки даних – це необхідність шифрування таких даних при їх обробці. З цим пов'язаний кейс Knuddels.de. Як пише Томас Фолтін у своїй статті: «Сайт для знайомства та спілкування, який є одним із найбільших в країні, *(йдеться про Німеччину – прим. Дейнека Є.)* повідомив у вересні наглядові органи, що 1,87 мільйона імені користувачів/паролів та понад 800 тис. адрес електронної пошти користувачів було скинуто на Mega.nz та Pastebin.com» [106].

Зрозумілим є те, що в даному випадку наглядовий орган Німеччини (йдеться не про BFDI, а про наглядовий орган однієї з німецьких земель) при розгляді справи знайшов порушення з боку компанії щодо забезпечення безпеки даних. Водночас варто відзначити, що він наголосив на тому, що: «Knuddels залишила персональні дані користувачів незашифрованими, надаючи зловмисника вільний доступ до інформації» [107].

Таким чином, можна зробити висновок про те, що якщо персональні дані незашифрованими, це є вагомим аргументом зі сторони наглядових органів, в контексті доведення, що контролер чи оператор не вживали заходів для забезпечення безпеки таких персональних даних.

2.2 Технологічні виклики у сфері захисту персональних даних

2.2.1 Захист даних при поширенні таргетованої реклами

Цієї частиною моєї роботи, я маю на меті аналізи основних проблем, які, на мій погляд, стали вже сьогодні чи стануть у найближчому майбутньому викликом для сфери захисту персональних даних. Такі виклики пов'язані здебільшого з розвитком інформаційних технологій та постійним розвитком засобів обробки та цілей для можливого використання персональних даних.

З огляду на це, для сучасних нормативно-правових актів важливо забезпечення мобільності і гнучкості. Подібні намагання закладені і в самому

GDPR. Підтвердженням цьому є, наприклад, достатньо широке визначення поняття «Персональних даних» та інших термінів, які запропоновані GDPR.

Відповідно основною моєю метою в цій частині роботи буде визначення, особливостей взаємодії GDPR з такими специфічними сферами, які є потенційно не мають однозначності щодо обробки персональних даних.

Першою сферою для аналізу в межах цього розділу, я обрав сферу таргетованої реклами. Ця сфера на сьогодні набуває надзвичайного поширення, в той же час є надзвичайно небезпечна, оскільки неймовірним чином впливає на людей.

Прикладом для цього може стати кейс канадської компанії Aggregate IQ. Справа розглядалася ICO після отримання ним інформації про те, що вказана компанія могла впливати на результати референдуму щодо виходу Великої Британії зі складу Європейського Союзу. В ході розгляду справи також було з'ясовано, що ця компанія також могла впливати на президентські вибори у США, коли там було обрано Дональда Трампа[108].

Цей кейс тісно пов'язаний з гучним скандалом щодо витоку персональних даних між Facebook та Cambridge Analytyca. Aggregate IQ отримував персональну інформацію про користувачів Facebook і в подальшому надсилав їм таргетовану рекламу щодо тих чи інших кампаній [109]. Таким чином особи отримували лише тут інформацію, яка була вигідна замовникам послуг компанії.

Такі звинувачення звучали достатньо шокуюче. Цей приклад показує, що таргетована реклама може впливати на великі групи осіб, фактично не залишаючи особам вибору в окремих ситуаціях. Порушення прав людини в такому випадку здається очевидним.

Подібної логіки дотримувався інший технологічний гігант. На початку 2020 року корпорація Apple заявила, що змінить правила доступу користувачів до окремих додатків, зокрема до Facebook. Один із новинних ресурсів цитує пост у Twitter генерального директора Тім Кука, де він пише наступне: «Ми впевнені, що користувачі повинні мати право вибору щодо зібраних про них даних і способів їх використання. Facebook як і раніше може продовжувати відстежувати

користувачів в додатках і на вебсайтах, просто прозорість відстеження додатків в iOS 14 запитає, щоб вони спочатку запросили ваш дозвіл» [110].

Ця заява переросла в скандал, який набув неосяжних масштабів та надзвичайного розголосу і навіть призвів до судових позовів від Facebook щодо порушення конкурентного законодавства [111].

Ці два приклади належним чином демонструють увагу сучасного суспільства до етичності та доцільності використання таргетованої реклами. Водночас варто відзначити, що таргетована реклама не є однозначним негативним явищем. Існують непоодинокі думки про беззаперечну користь таргетованої реклами. Так, наприклад, Ден Голден у своїй статті пише про те, що: «Якісно зроблена таргетована реклама, дозволяє отримувати лише актуальну рекламу перед очима. Бренди контактують зі споживачами, які бачать рекламу лише товарів в яких вони зацікавлені» [112].

Таким чином, неможливо стверджувати, що таргетована реклама відійде чи буде відкинута суспільством, як однозначно негативне явище. З огляду на це, важливо з’ясувати, що саме являє собою таргетована реклама та яким чином вона взаємодіє з обробкою персональних даних.

Очевидним є те, що оскільки таргетована реклама не є правової категорії, в законодавстві ніколи не зустрічається її визначення. Водночас окремі юристи-практики наступним чином описують таргетовану рекламу: «Таргетована реклама – різновид діджитал-маркетингу (полягає в показі клієнту найрелевантніших рекламних оголошень, підібраних на основі дослідження його попереднього досвіду, уподобань, інтересів)»[113].

Є і більш, узагальнені визначення, як, наприклад, «Форма реклами в Інтернеті, яка фокусується на конкретних рисах, інтересах та уподобаннях споживача. Рекламодавці отримують цю інформацію, відстежуючи вашу активність в Інтернеті» [114].

Так чи інакше, вже ці визначення дають уявлення про об’єми персональних даних, які обробляються в ході розробки такої реклами. Оскільки

аналіз робиться на основі інтересів та вподобань клієнтів, їх необхідно детально вивчати протягом певного проміжку часу.

Як зазначають інформаційні ресурси, «Рекламні платформи можуть збирати дані з різних джерел. Найпоширеніші з них – це файли cookie на вебсайтах, які ви переглядали. Файли cookie – файли, які зберігають інформацію про ваші дії або покупки на сайті та передають їх до CRM або сторонніх організацій» [115].

З регулювання використання таких файлів, ми стикалися при аналізі законодавства держав членів ЄС. Зокрема, окреме правове регулювання для використання cookie-файлів передбачено у Великій Британії, Іспанії та Німеччині. Це зрозуміло, з огляду на те, що в самому GDPR cookie-файлам приділено небагато уваги.

Параграф 30 GDPR передбачає, що: «Фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою … ідентифікаторів «cookie» (реп’яшків) або інших ідентифікаторів … . Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації» [3].

Вказане свідчить про те, що в GDPR обґрунтовано наявність небезпеки використання персональних даних при використанні таких файлів. Водночас GDPR не містить заборон на використання таких файлів. Це зрозуміло, з огляду на те, що такий підхід абсолютно зруйную сферу таргетованого маркетингу, яка є «зручним способам отримання інформації про потенційно цікаві продукти» [115] майже для кожної третьої особи [115].

В той же час, параграф 10 GDPR містить інформацію про те, що цей «Регламент не виключає законодавство держави-члена у визначенні обставин особливих ситуацій опрацювання, зокрема в уточненні умов, за яких опрацювання персональних даних є правомірним» [3]. Відповідно це пояснює те, що окремі держави-члени ЄС врегульовують певні аспекти використання таких файлів в межах національного законодавства.

Водночас питання таргетованої реклами так само можна розглядати зі сторони законності та отримання дозволу на опрацювання персональних даних, що відбувається в межах GDPR.

Стаття 4 GDPR передбачає, що «згода суб'єкта персональних даних означає будь-яке вільно надане конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних» [3]. Тобто, як мінімум, суб'єкт даних повинен бути поінформований про те, що здійснюється обробка його персональних даних, а в з урахуванням положень статей 6 та 32 GDPR, можна стверджувати, що суб'єкта повинно бути повідомлено, що в тому числі і той факт, що для обробки персональних даних використовують cookie-файли.

Крім того, в роз'ясненнях EDPB міститься пояснення, що: «Послуга може включати кілька процесів обробки з більш ніж однією метою. У таких випадках, суб'єкти даних повинні вільно обирати, щодо яких цілей вони дозволяють обробку, замість того, щоб давати згоду на весь перелік цілей обробки» [116].

Тобто особа повинна мати можливість відмовитися від використання щодо неї cookie-файлів і відповідно відмовитися від таргетованої реклами, яка є неможливою без використання цих файлів. Подібну можливість, надає корпорація Apple для користувачів своїх смартфонів в рамках вже описаних нижче нововведень.

Крім того, варто зауважити, що на контролерів даних так само покладається відповідальність щодо збереження конфіденційності цих персональних даних. Водночас, варто відзначити, що GDPR не є єдиним документом на рівні ЄС, який спрямований на врегулювання питання таргетованої реклами. В цьому контексті також варто говорити Директиву про обробку персональних даних та захист конфіденційності в секторі електронних комунікацій 2002/58/ЄС [117].

Підхід сформований у GDPR є найбільш оптимальним виходом в даній ситуації. Таргетована реклама на сьогодні є невід'ємним інструментом в

маркетинговій діяльності. Водночас об'єми обробки персональних даних є надзвичайними, що повинно збалансовуватися можливістю кожного суб'єкта даних самостійно робити вибір щодо застосування таргетованої реклами щодо себе.

2.2.2. Суперечності між технологією блокчейн та захистом даних за GDPR

Технологічний розвиток сучасного світу досягає нового рівня повсякчас. У фінансовій сфері втіленням цього процесу стало поява першої криптовалюти – Bitcoin у 2009 році [118].

Водночас поява перших криптовалют привернула увагу також до технологій, що використовуються для їх створення – блокчейну. Ці технології, як і обіг криптовалют, і сьогодні не отримали достатньої оцінки з правової точки зору. Більшість країн світу не мають правового регулювання для обігу криптовалют взагалі або застосовують різні концепції до регулювання такого обігу.

Водночас відразу після прийняття GDPR, через підвищену увагу до криптовалют в той період, досить швидко постало питання про співставність GDPR і технології блокчейн. Про це зазначає, European Parliamentary Research Service (далі – «**EPRS**») у своєму брифінгу до великого дослідження «Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with Eroupean data protection law», яке було проведено у 2019 році. [119].

Зокрема EPRS зазначає, що: «Існує значне напруження між сутністю технології блокчейну та загальною структурою Загального регламенту захисту персональних даних» [119].

Їх співіснування пов'язане з цілим рядом проблем. Зокрема, в практичній сфері виділяють наступні: «Що насправді вважати персональними даними в блокчейні? … Хто є контролером персональних даних, оператором персональних даних, або спільним контролером? … Право бути забути. … Хто

несе відповідальність за порушення? …. Чи можна зашифровані персональні дані зберігати на блокчейні?» [120]. Тобто проблемні питання у співвідношенні блокчейну і GDPR виникають навіть щодо найпростіших та фундаментальних питаннях сфери захисту персональних даних.

Враховуючи, що протягом останніх років, увага як до сфери захисту персональних даних, так і до сфери використання технології блокчейн, є стабільно високою, вирішення вказаних вище проблем є одним з найбільших викликів як для захисту персональних даних загалом, так і для GDPR, зокрема.

З огляду на це, варто з'ясувати в чому сутність технології блокчейн. Однакового визначення технологій блокчейн немає. Так, в одних випадках пишуть про те, що: «Блокчейн – це своєрідна база даних у якій дані зберігаються і розподілені між великою кількістю вузлів (комп'ютерів) та записи про які доступні всім користувачам мережі» [121]. В інших джерелах, можна знайти інше визначення, наприклад: «Блокчейн – це спільна, незмінна реєстраційна книга для запису історії транзакцій» [122].

Ці визначення відразу дозволяють підтвердити вище наведені проблеми. Так, наприклад, якщо звернути уваг на те, що в блокчейні задіяні велика кількість вузлів, відразу виникатиме проблема з визначенням контролера даних, на якого буде покладати зобов'язання дотримуватися GDPR та відповідальність за його порушення. В той же час, незмінність, як характерна риса блокчейну, про яку згадано в другому із запропонованих визначень, відразу породжуватиме питання щодо можливості зміни інформації про особу чи дотримання права бути забути, які передбачені в GDPR. [3].

Водночас ці визначення не розкривають всю специфіку технології блокчейну. Так, юридичні радники технологічної компанії Bitfury Group та юристи української компанії Asters Юрій Котляров та Сергій Циба в своїй спільній статті пишуть про три основні проблеми, які виникають при застосуванні технології блокчейн на практиці: «Анонімізація особистих даних, ідентифікація та зобов'язання контролерів та операторів даних, права суб'єктів даних» [123].

Перше з цих питань, щодо анонімізації даних, можна пояснити тим, що відсутнє чітке розуміння, чи варто вважати персональні дані, що збираються в ході застосування технологій блокчейн анонімними. А це є важливим в контексті застосування GDPR, оскільки параграф 26 GDPR передбачає, що: Таким чином, цей Регламент не стосується опрацювання такої анонімної інформації, у тому числі для статистичних або дослідницьких цілей» [3]. Тобто, якщо можливо довести, що персональні дані, що обробляються в ході використання технології блокчейн є анонімними, можливо буде заперечити необхідність застосування GDPR.

Автори вже згаданої статті пишуть про те, що: «Протоколи блокчейну застосовують public-private-key cryptography, також відому як асиметрична криптографія, та криптографічні хеш функції» [123].

Обидва цих методи фактично шифруються інформації про особу, перетворюючи їх у набір символів, який фактично неможливо співставити з певної конкретною особою. На користь цих методів також говорять аргументи про унікальність коду в який перетворюється інформації при застосуванні технології блокчейну. [123].

Водночас автори наголошують на тому, що: «Поки існує obfuscation techniques, (технологія дозволяє проводити зворотній процес до процесу, що відбувається з використання асиметричної криптографії та криптографічні хеш функції, тим самим забезпечуючи дешифрування вказаних даних – прим. [123]), той факт, що можливо провести декомпіляцію хеш значення – важливий момент. Якщо це можливо, тоді це означає, що значення хеш-функції не є анонімними даними» [123].

У випадку з аналізом проблеми з визначенням контролера та обробника даних, варто зважати на існування двох видів блокчейну – публічного і приватного. Оскільки, «приватний блокчейн – базується на тих самих принципах, однак «адмініструється конкретними особами або корпоративно» [121], то визначення контролера персональних даних в такому випадку, більш передбачуване, це буде «адміністратор» блокчейну.

Натомість «публічний блокчейн – повністю децентралізований. У такому блокчейні відсутні особи, які володіють контролем над ним. Будь-яка особа може бачити транзакції та надсилати власні транзакції на підтвердження» [121]. В такому випадку, фактично неможливо визначити, хто саме обробляє персональні дані, оскільки кожен з учасників цього процесу перебуває на однаковому рівні можливостей щодо впливу на всі без винятку процеси.

Найбільш вірогідним виходом в такому випадку тут є застосування концепції, що передбачена статтею 26 GDPR: «Якщо два чи декілька контролерів спільно визнач ають цілі та засоби опрацювання, вони є спільними контролерами. Вони повинні на умовах прозорості встановити свої відповідні обов'язки, що відображають зміст зобов'язань за цим Регламентом» [3].

Водночас застосування цієї статті викликає і окремі запитання, зокрема Cristian Wirth та Michael Kolain у своїй статті пишуть про: «Поки залишається незрозуміло чи обов'язок … статті 26 GDPR, є причиною, яка дозволяє стверджувати про наявність спільного контролю, чи навпаки є наслідком спільного контролю» [124].

В той же час, навіть визначення контролера в таких відносинах не ставить остаточної крапки щодо можливості здійснення своїх прав суб'єктами даних, оскільки публічні блокчейни «розділені між кількома географічними локаціями. Ці локації не є ні заздалегідь визначеними, ні фіксованими» [123]. Відповідно, визначення конкретної особи, до якої варто звертатися для виправлення чи видалення персональних даних буде становити складність для суб'єктів даних.

В той же час, непоодинокими є думки про те, що технології блокчейн можуть стати надзвичайними важливими і корисними для сфери захисту персональних даних. Так, IBM наводить у своїх інформаційних матеріалах наводить безліч прикладів щодо того, як саме можна застосовувати блокчейн для захисту персональних даних, серед яких ідентифікація пасажирів при пересадках між рейсами в різних країнах та ідентифікації укладення договорів купівлі-продажу до відстеження надання згоди суб'єктами даних [122].

Загалом варто відзначити, що для визначення всіх переваг і недоліків існування та використання технологій блокчейну та співставлення з захистом персональних даних, все таки не вистачає визначеності в правовому регулюванні блокчейну, який дасть відповіді на безліч неоднозначних питань, які постають на сьогодні.

2.2.3 Захист персональних даних у соціальних медіа

Соціальні медіа в сучасному суспільстві є невід'ємною його складовою. Фактично на сьогодні все складніше знаходити людей, які ніяким чином не перетинаються з соціальними медіа щоденно.

Варто зауважити, що для цілей цього підрозділу, я умисно вживаю не термін «соціальні мережі», а саме «соціальні медіа». Це пояснюється тим, що в рамках цієї частини роботи, я маю намір вийти за межі виключно обробки персональних даних в соціальних мережах.

Як зазначає Radi Petrov Romansky у своїй статті: «Термін «соціальні медіа» описує комплекс різних інтернет та мобільних технологій, які дозволяють перетворити комунікацію в інтерактивний діалог та обмін картинками, аудіо та відеофайлами, досвідом, тощо» [125].

В такому контексті, на мій погляд, варто говорити про обробку персональних даних в цій тематиці. Тобто, не тільки в соціальних мережах, але і на відкритих форумах, платформах для обговорення, сайтах для пошуку роботи чи в додатках та комп'ютерних іграх. Все з вищезгаданого об'єднує те, що вони використовують персональні дані своїх користувачів, а також, що таким чином, люди можуть спілкуватися між собою. Навіть, у комп'ютерних іграх, здавалося б максимально відділених від спілкування між людьми, кожен може писати текстові повідомлення один одному. Це свідчить про наявність комунікації між людьми і свідчить про схожі між іграми і соціальними медіа – ми використовуємо їх в різних цілях, але однаково має здатність спілкуватися і в іграх, і в соціальних мережах.

Варто також відзначити, що в цій частині роботи, я не зачіпатиму проблематику використання персональних даних в таргетованій рекламі, яка, як можна побачити зі справи Facebook, тісно пов'язана зі сферою персональних даних. [126]

В контексті розвитку цієї тематики, варто зауважити, які саме персональні дані опрацьовуються чи задіються при використанні соціальних медіа. Згідно зі статтеюі 4 GDPR персональні дані: «означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, … онлайн-ідентифікатор» [3].

Таким чином в поняття персональних даних вводиться IP-адреса пристрою та інші технічні ідентифікатори пристроїв. Водночас виникає питання, чи можливо розглядати, як персональні дані нікнейм в соціальних медіа.

Антон Тарасюк у своїй статті пише про те, що: «З одного боку – наявність інформації, що користувач «Білий Вепр» зареєстровано за таким ніком, може здатися незначною і такою, що не передбачає обробку його персональних даних. Однак, цей нікнейм може ставати онлайн-ідентифікатором в рамках GDPR, який дозволяє відокремити цього користувача від інших і, відповідно, такий нікнейм буде персональними даними» [127].

GDPR не передбачає окремих положень про використання нікнеймів. Водночас GDPR передбачає можливість «використання псевдонімів», що означає: «опрацювання персональних даних у такий спосіб, що персональні дані більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації за умови, що таку додаткову інформацію зберігають окремо і на неї поширюється застосування технічних і організаційних інструментів для забезпечення того, що персональні дані не віднесено до фізичної особи, яку ідентифіковано чи можна ідентифікувати» [3].

Псевдонімізація персональних даних вже згадувалася у попередніх частинах роботи, як засіб забезпечення більшої безпеки даних. Водночас у

випадку застосування цієї категорії даних щодо нікнеймів, можна стверджувати, що нікнейми будуть в загальному відповідати ознакам, які вкладаються у цитоване вище поняття (наявна додаткова інформація, зберігається така інформація окремо і т.д.). Опираючись на це, можна стверджувати, що нікнейм, що використовується в соціальних медіа варто розглядати, як персональні дані для GDPR.

Іншим наочним прикладом небезпеки при опрацюванні персональних даними є політики конфіденційності – Privacy Policy. До набрання чинності GDPR це були об'ємні документи, які містили безліч складних конструкцій чи, як мінімум, професійних юридичних термінів, які не завжди, були тим хто їх читав. В той же час, читали такі політики достатньо рідко, просто проставляючи позначку про прийняття умов цієї політики.

З GDPR все змінилося. Секція 1 та 2 Глави другої GDPR містять вимоги щодо політики опрацювання персональних даних, які можна узагальнити положеннями статті 12, яка передбачає, що: «Контролер повинен вжити необхідних заходів для надання будь-якої інформації, … щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння та легко доступній формі, з використанням чітких і простих формулювань» [3].

Таким чином, GDPR вимагає від контролерів наявності короткого та зрозумілого документу, замість попередніх політик. Варто зауважити, що Політика має бути зрозуміла кожному, що перекликається з аналізованим у попередній частині роботи кейсом щодо порушення положень GDPR тенісною асоціацією Нідерландів, де ситуація була у тому, що не було доведено цілей опрацювання персональних даних до всіх учасників асоціації.

Близьким до цього контексту, є умови статті 7 GDPR щодо надання згоди на обробку персональних даних. Зокрема, частина 3 статті 7 передбачає: «Запит на надання згоди необхідно подавати у формі, що чітко відрізняється від інших питань, у зрозумілій та доступній формі, з використанням чітких і простих формулювань» [3].

Разом, політика конфіденційності та правила надання згоди, повинні стати основою безпечності персональних даних в соціальних медіа. Водночас це не розв'язує інші питання, як, наприклад, мінімізація даних та забезпечення їх безпеки.

Одним із принципів GDPR звучить наступним чином: «вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання («мінімізація даних»)»[3]. Водночас як пише вже цитований мною Radi Petrov Romansky: «Традиційне визначення терміну «приватність», як «право бути наодинці», і цей сенс слід зберігати має зберігатися при глобальних контактах через соціальні мережі» [125].

Водночас варто враховувати, що приватність у соціальних мережах дещо деформоване поняття, оскільки складно уявити, яким чином контролер персональних даних може контролювати, які персональні дані поширюються користувачами у соціальних медіа. Хтось буде заповнювати тільки прізвище, ім'я, інші додатково можуть поширювати – вік, стать, професію і т.д. Виникає питання, чи повинна захищати персональні дані, які не є обов'язковими для заповнення користувачами і яким чином повинні пояснювати цілі їх обробки. Це запитання на які GDPR, не містить однозначної відповіді на ці запитання.

Ще однією не до кінця вирішеною складністю в щодо соціальних медіа та захисту персональних даних дехто виділяє співвідношення авторського права та захисту персональних даних.

Про це, наприклад, пише Rebecca Trussell у своєму блозі на сайті уряду Сполученого Королівства. Зокрема, вона наводить приклад фотографів, які: «хочуть поширити для публіки свої фото, щоб розвивати свій бізнес та поширювати свої найкращі витвори» [128].

Водночас з урахування того, що персональні дані за GDPR включають також фізіологічні та генетичні ідентифікатори [3]. Відповідно при поширенні фотографії в соціальних мережах, потрібно враховувати, що вона містить персональні дані осіб, що зображені на цьому фото. Rebecca Trusell пише про те,

що при поширенні фотографій потрібно дотримуватися GDPR та отримувати згоди від осіб на фото [128].

Складність полягає у визначенні необхідності з боку соціальної мережі, де поширюється така фотографія відстежувати дотримання GDPR в такому випадку.

З огляду на вищесказане, варто відзначити, що обробка персональних даних в соціальних медіа за GDPR набула змін і була однозначно вдосконалена. Водночас залишається невиключний перелік питань, які не знайшли однозначного вирішення в GDPR.

2.3 Особливості захисту персональних даних в рамках Ради Європи

2.3.1 Правові основи та підґрунтя захисту персональних даних в рамках Ради Європи

Проблемам захисту персональних даних у Європі приділено уваги не лише в рамках Європейського Союзу. Навіть, до ЄС, сфера захисту персональних даних мала правове регулювання в рамках Ради Європи.

Підґрунтя цьому регулюванню містила стаття 8 Європейської конвенції про захист права та основоположних свобод людини та громадянина (далі – «**ЄКПЛ**» або «**ECHR**»), якою передбачено «право на повагу до приватного та сімейного життя» [3]. Подальший розвиток захист персональних даних в рамках Ради Європи знайшов своє відображення в інших нормативно-правових актів, які було прийнято протягом другої половини двадцятого століття. Тобто, в той же час, що і розвиток правового регулювання персональних даних у ЄС, який привів до прийняття GDPR.

З огляду на цей факт, а також достатньо схожу територію дії двох механізмів захисту персональних даних – GDPR та ECHR, доцільним є, на мій погляд, аналіз співвідношення цих механізмів та порівняння окремих аспектів їх дії в контексті схожих обставин.

Правову основу захисту персональних даних в рамках Ради Європи, крім ЄКПЛ, так само забезпечено Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року, так звану Конвенцію 108 [129], та Додатковим протоколом до цієї Конвенції, який прийнято 8 листопада 2001 року.

Якщо останні два документи безпосередньо спрямовані на регулювання сфери захисту персональних даних, то ЄКПЛ не містити в собі згадок про персональні дані. Стаття 8, порушення якої розглядається при заявах щодо захисту персональних даних, передбачає, що: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [3]. Частина друга цієї статті містить обмеження повноважень державних органів щодо здійснення втручання в приватне життя осіб [3].

Їх захист передбачений статтею 8, оскільки: «Суд дав широке визначення обсягу статті 8, навіть якщо певне право не перелічене у цій статті» [130]. Тобто, як і багато інших прав, право на захист персональних даних знаходить своє відображення в ЄКПЛ тільки завдяки практиці Європейського суду з прав людини (далі – ЄСПЛ). Як зазначено у посібнику Ради Європи щодо використання ЄКПЛ: «Те, що дає ЄКПЛ сили і робить її надзвичайно сучасною – це тлумачення її ЄСПЛ: динамічно, з урахуванням сучасних умов»[131].

З цього слідує, що невід'ємною складовою аналізу механізму захисту персональних даних в рамках Ради Європи, є ознайомлення з судовою практикою ЄСПЛ, яке є проведу в наступній частині моєї роботи.

Водночас Конвенція 108 та Додатковий протокол до неї були результатом розвитку практики захисту персональних даних. Як зазначає ряд науковців, зокрема Бем М.В., Городинський І.М., Саттон Г. та Родіоненко О.М. у своїй книзі: «Ключові положення вказаних рішень Європейського суду з прав людини (*йдеться про рішення ЄСПЛ у сфері захисту персональних даних, які згадуються авторами попередньо – прим. Дейнека Є.*) лягли в основу прийнятої 28 січня 1981 року Конвенції № 108… Цей документ став першим у цій сфері. У ньому вперше викладено ключові принципи обробки персональних даних, права особи у

зв’язку з обробкою персональних даних, базові норми для транскордонної передачі даних» [132].

Тобто Конвенцію 108 і Додатковий протокол варто розглядати, як джерело, яке є результатом розвитку сфери розвитку сфери персональних даних у XX століття. Водночас варто зауважити на специфіку сфери дії Конвенції, яка є вужчою ніж сфера дії за GDPR.

Зокрема, в контексті конвенції йдеться виключно про «файли персональних даних для автоматизованої обробки та до автоматизованої обробки персональних даних у державному та приватному секторі» [3]. З огляду на це, варто зазначити, що в розумінні Конвенції, автоматизована обробка являє собою: «операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних та (або) арифметичних операцій із цими даними, їхню зміну, знищення, вибірку або поширення» [3].

Тобто сфера застосування Конвенція є дещо вужчою і не охоплює опрацювання персональних даних, що здійснюється неавтоматизованим чином, як це передбачає GDPR. Це зрозуміло, з огляду на те, що: «Із появою у 1960-их роках інформаційних технологій з’явилася потреба у розробленні більш детальних правил забезпечення захисту осіб через охорону їхніх (персональних) даних» [129]. Тобто Конвенція стала відповіддю на нові виклики пов’язані з зародженням та бурхливим розвитком сучасних інформаційних технологій.

Водночас на відмінну від GDPR, який мати імперативний характер для держав-членів ЄС, Конвенція дозволяє диспозитивність для держав-сторін Конвенції щодо поширення дії Конвенції, дозволяючи державам обирати категорії даних щодо яких застосовується Конвенція і можливість застосування цієї Конвенції до неавтоматизованої обробки [3].

Як і для GDPR, надзвичайно важливим аспектом Конвенції 108 є принципи обробки персональних даних, які багато в чому співзвучні з принципами Регламенту: законна обробка, визначення цілей обробки, адекватність та ненадмірність, точність та оновлюваність [3]. З цього слідує, що такі принципи

обробки персональних даних викристалізувалися достатньо давно і їх формування не пов’язане виключно з GDPR.

Окремі аспекти відрізняють Конвенцію та GDPR в аспекті визначення контролерів та операторів персональних даних. Зокрема у вже цитованому мною посібнику автори пишуть про те, що: «Якщо компанії входять до складу групи, компанія-засновник і кожна філія, які є самостійними юридичними особами, вважаються окремими володільцями або розпорядниками. Такий самостійний правовий статус кожного члена групи виливається у необхідність існування спеціалізованої правової бази, яка б дозволила взаємну передачу персональних даних» [129].

Водночас Конвенція не передбачає можливість розглядати кількох контролерів разом в окремих ситуаціях, як це передбачено у GDPR, зокрема, щодо спільних контролерів і можливості призначати єдиного Data protection officer для групи компаній.

Варто звернути увагу і на достатньо «обмежений» термінологічний апарат, який послуговується Конвенція. Зокрема, наприклад в ній не закріплено визначення поняття «згоди на обробку персональних даних» та вимог щодо нього, яка, як передбачено у Посібнику: «є такими самими, що й для незаперечного волевиявлення, закріпленого у європейському цивільному праві» [129]. Водночас Конвенція міститься достатньо дивне на сьогодні, на мій погляд, визначення поняття «файл даних для автоматизованої обробки», що означає «будь-який масив даних, що піддається автоматизованій обробці» [3]. Це визначення є важливим в контексті того, що воно використовується Конвенцію досить часто у випадках, де було більш доцільно, використовувати термін «персональні дані». На мою думку, цей термін є дещо застарілим і не зовсім відображає сутність інформації, що обробляється при обробці персональних даних, оскільки використовує інші поняття, наприклад, «файл», які потребують додаткового уточнення.

Кілька слів варто сказати про інші категорії, які аналізувалися мною в першій частині роботи, де деталізувалися окремі частини GDPR. Перш за все

варто звернути увагу на діяльність наглядових органів, оскільки: «Незалежний наглядовий орган виявився незамінним для розвитку ефективного захисту персональних даних» [129], тенденції до створення повноправних наглядових органів починали з'являтися вже на початку XXI століття. Це підтверджує Додатковий протокол до Конвенції 108, яким було змінено специфіку діяльності наглядових органів.

Якщо першочергово кожна держава формувала органи, діяльність яких була спрямована на захист персональних даних з більш ознайомлювальною метою та для забезпечення співробітництва між державами, то Протокол спрямований на зобов'язання держав на створення саме наглядових органів, повноваження яких будуть включати саме контроль за належною обробкою персональних даних.

Так, наприклад, пункт 2.а. Статті 1 Протоколу передбачає: «Для цього зазначений вище орган нагляду має, зокрема, повноваження стосовно розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права» [3].

Крім того, преамбула Протоколу згадує про те, що такі наглядові органи повинні «виконувати свої функції в повній незалежності»[3]. Хоча, варто зауважити, що в GDPR питанням незалежності наглядових органів та забезпечення їх діяльності приділено більше уваги, ніж в цьому Протоколі, все ж створення і діяльність незалежних і цілком повноважних наглядових органів є тенденцією, яка послідовно розвивається на теренах Європи вже понад двадцять років.

Так само варто зазначити, що Конвенція, як і GDPR, дозволяє країнам створювати кілька наглядових органів, проте без зобов'язання визначення одного контролюючого органу, який уповноважений діяти від імені держави [3]. Водночас Конвенція ніяким чином не розв'язує питання взаємодії між контролерами та наглядовими органами при діяльності в різних державах, як це зроблено в GDPR завдяки концепції LSA. Ймовірно, це варто пояснити тим, що

наднаціональну правову систему в ЄС та правові документи Ради Європи не ефективно порівнювати з точки зору взаємодії між державами, оскільки в ЄС, вона буде більшою, вже виходячи із цілей створення Союзу.

Окремим аспектом, ще варто зауважити про відповідальність. Стаття 10 Конвенції передбачає, що: «Кожна Сторона зобов'язується встановити відповідні санкції та засоби правового захисту стосовно порушень положень внутрішнього права, що запроваджують основоположні принципи захисту персональних даних» [3].

Тобто, з цього слідує, що Конвенція пише про відповідальність достатньо коротко, відносячи до питання національного законодавства держав-сторін Конвенції. Про те, така обмежена риторика щодо відповідальності не завжди ефективно спрямовує національне законодавство. Прикладом, можна взяти Україну, яка приєдналася до Конвенції, але не є членом ЄС, відповідно на неї не поширюються положення про відповідальність за GDPR. Штрафи, передбачені законодавством нашої країни, мізерні в порівнянні із санкціями передбаченими за порушення GDPR, які водночас є достатньо гнучкими.

Водночас Конвенція, як і GDPR, передбачає створення консультативного органу на міжнародному рівні. В рамках Ради Європи – це Консультативний комітет, який формується з представників від держав-сторін Конвенції, подібним чином до GDPR [3].

Крім того, як і в GDPR, у Конвенції йдеться виключно про сферу накладення санкцій на суб'єктів, що здійснюють обробку персональних даних. Водночас оминається питання відшкодування шкоди для суб'єктів даних чиї права було порушено.

З огляду на вищесказане, варто зауважити, що механізми захисту персональних даних в рамках Ради Європи та Європейського Союзу є достатньо схожими і має однакові витоки. Про таку схожість можна говорити в контексті принципів обробки даних, та тенденціях до створення наглядових органів та особливостях регулювання передачі даних.

Водночас наявні і різкі відмінності між двома підходами до регулювання сфери, що розглядається. Ймовірно, це варто пояснювати достатнім часовим проміжком між прийняттям нормативно-правових актів в Раді Європи та Європейському Союзі.

Важливо також зазначити, що велику увагу в рамках Ради Європи варто приділяти практиці ЄСПЛ, яка буде більш детально проаналізована в наступній частині.

2.3.2 Практика Європейського суду з прав людини у справах щодо захисту персональних даних

Як зазначалося вище, аналіз сфери захисту персональних даних в рамках Ради Європи, зокрема в контексті статті 8 Європейської Конвенції про захист основоположних прав і свобод людини і громадянина, об'єктивно неможливий без аналізу окремих рішень ЄСПЛ, в яких ЄСПЛ деталізує тлумачення права на приватність та захист персональних даних.

Оскільки, як з'ясовано у минулій частині роботи, захист персональних даних в рамках Ради Європи та ЄС мають певні відмінності, аналіз судової практики ЄСПЛ є необхідним для повноти вирізнення таких відмінностей.

Відразу варто відзначити, що ЄСПЛ при розгляді справ, що стосуються порушення у сфері захисту персональних даних розглядає конкретні справи у взаємодії трьох критеріїв, про які пишуть Владислав Власюк та Аліна Куц-Карпенко: «Щоб вирішити, чи втручання держави в право людини на приватність є законним, потрібно «пройти» трискладовий тест – чи таке обмеження «втручання): відповідає закону; переслідує законну мету; а також є необхідним у демократичному суспільстві для досягнення законної мети» [133].

Варто відзначити, що такий тест притаманний не лише для справ пов'язаних з обробкою персональних даних, а для будь-яких категорій справ, де розглядається порушення статті 8 ЄКПЛ.

Аналіз окремих кейсів варто почати, на мій погляд, з кінця. Одне з останніх рішень ЄСПЛ, яке було ухвалено у 2021 році стосується використання персональних даних в Угорщини. У справі L.B. v. Hungary, ЄСПЛ розглядав правомірність поширення відомостей про особу. Як зазначає в пунктах 4-8 Рішення у справі, де викладені обставини справи, податкові контролюючі органи використовували персональні дані особи при формуванні списку неплатників податків. Вказані персональні дані були використані в інтернет медіа, яка створювала карту неплатників податків у країні. Таким чином особа, чиї дані було поширено вважала, що її дані використовувалися незаконно [134].

Незважаючи на достатньо контраверсійні позиції сторін у справі, зокрема позиції скаржника про те, що: «Головною метою оприлюднення його персональних даних у списку неплатників податків був публічний осуд, який не може вважатися легітимною метою відповідно до статті 8 Конвенції»[134], та позиції уряду Угорщини, яка стверджувала: «Що втручання мало легітимну мету – захист економічного добробуту країни та прав інших осіб» [134], ЄСПЛ визнав наявність такої законної мети, оскільки оприлюднення таких даних було передбачено законодавством Угорщини [134].

Водночас ЄСПЛ в контексті питання про обсяг оприлюднених даних. також звернув увагу на те, що: «Публікація списків неплатників податків була б безглуздою, якби не виникало можливості ідентифікувати конкретного платника податків» [134]. Отож, в такому випадку ЄСПЛ фактично не залишив достатньо широкі рамки для інформації, що може поширюватися в такому випадку, оскільки критерій «можливості ідентифікації» фактично не залишає жодних обмежень, крім об’єктивно неспівставної з цієї метою інформації.

Все ж, підкріплюючи свою позицію аргументом, що: «Лише факт, що доступ до переліку не був обмежений, не означає, що на список звертало увагу суспільство» [134], ЄСПЛ визнав відсутність порушення в такому випадку.

В контексті розгляду цієї справи з ретроспективою на GDPR, хотів би зауважити два окремих моменти. Перш за все, в рамках даної справи не розглядалася законність використання оприлюднених персональних даних

інтернет медіа. Хоча, за даних обставин, на мій погляд, ця ситуація могла б розглядатися наглядовими органами Угорщини в контексті порушення законності обробки персональних даних та умов надання згоди на таку обробку, тобто статей 6 і 7 GDPR [3].

Інший аспект, на якому, я хотів би наголосити, це один із аргументів заявника по справі, де він стверджував: «Що уряд не продемонстрував, що запит на підставі статті 14 (c) Закону про захист персональних даних був ефективним засобом захисту… видалення персональних даних на підставі цієї норми можна скористатися лише у випадках незаконної обробки» [134]. Такі положення законодавства Угорщини суперечать положенням статті 16 та 17 GDPR, які передбачаються можливість суб'єктів даних на виправлення персональних даних про себе та «право бути забутим» [3].

Наступним кейсом, який буде мною аналізований, є справа Авілкіна та інші проти Російської Федерації, де розглядалася правомірність поширення медичних відомостей про осіб правоохоронним органам [135]. За обставинами справи російська прокуратура збирала інформації про переливання крові особам, які належать до релігійної організації свідки Єгови (така увага до конкретної організації спричинена заявою Комітету з порятунку молоді від деструктивних культів та віруваннями організації, які забороняли переливання крові) [135].

Як зазначали заявники: «Запитувана прокуратурою інформація належала до конфіденційної медичної інформації і підпадала під захист передбачений статтею 8 Конвенції. Така інформація була передана від медичних установ до прокуратури без їх згоди» [135].

В контексті розгляду цієї справи ЄСПЛ заявив, що «положення, … щодо про випадки допустимості розкриття конфіденційної медичної інформації були передбачені були сформульовані в досить загальних рисах» [135]. Тобто, ЄСПЛ однозначно висловлює свою позиції щодо необхідності чіткого врегулювання підстав для збору такої інформації державними органами, що перегукується з положеннями статті 5 та 6 GDPR, які обґрунтовують необхідність наявності законної мети та захисту важливих інтересів третіх сторін [3].

Крім того, визнаючи порушення статті 8 в цій справі, ЄСПЛ також зазначив, щодо того, що: «Перебування медичної інформації в прокураторі, не давали заявникам достатнього захисту від несанкціонованого розкриття» [135]. Тобто так само як і в GDPR, так і в практиці ЄСПЛ наявні чіткі тенденції щодо покладення на контролерів персональних даних зобов'язань щодо вжиття заходів для запобігання незаконному розкриттю інформації.

В контексті тлумачення поняття «персональних даних» цікавим є рішення ЄСПЛ у справі S. і Marper проти Сполученого королівства. За обставинами справи можна визначити, що розглядалася заява осіб, яких було виправдано щодо обвинувачень у вчиненні ними злочинів, однак відмовлено у знищенні даних, що збиралися про цих осіб – зразків відбитків пальців, ДНК профілів та зразків клітин [136]. Основним аргументом уряду Сполученого королівства полягав у тому, що: «Виключно зберігання відбитків пальців, профілів ДНК та зразків клітин для обмеженого використання … не підпадає під сферу дії права на повагу до приватного життя, передбаченого статтею 8» [136]. Проте ЄСПЛ визнав порушення статті 8 ЄКПЛ виходячи з дисбалансу між інтересом щодо збереження конфіденційності персональних даних та інтересами щодо , зазначивши: «Загальний і невибірковий характер повноважень щодо зберігання відбитків пальців, клітинних зразків та профілів ДНК осіб, яких підозрювали, але не засудили за вчинення злочину… не відповідає справедливому балансу між протидіючими суспільними та особистими інтересами» [136].

Так само, в рамках цієї справи ЄСПЛ вкотре наводить свою позицію, щодо визначення меж терміну «приватне життя», який, на думку ЄСПЛ: «Є широким терміном, що не піддається вичерпному визначенню» [136] В продовження цієї думки ЄСПЛ згадує різноманітні сфери, які мають відношення до приватного життя, з огляду на попередні судові рішення – фізичну, психічна цілісність, фізична та соціальна ідентичність, гендерна ідентичність, ім'я, сексуальна орієнтація та статеве життя, інформація про здоров'я особи і т.д. [136].

В контексті розуміння поняття «персональних даних», про який я писав перед описом цього кейсу, важливо зазначити, що на національному рівні судові органи Сполученого Королівства не мали однозначної позиції щодо належності до персональних даних відбитків пальців, оскільки за словами цитованого у рішення судді Лорда Воллер: «Відбитки пальців та профілі ДНК виявляють лише обмежену особисту інформацію» [136]. Водночас така позиція була як не сприйнята ЄСПЛ, так і відкинута самим Сполученим Королівством у ході розгляду справи [136].

З огляду, на це варто відзначити, що ЄСПЛ включає до поняття персональних даних генетичні ідентифікатори особи. Водночас в рамках іншої справи ЄСПЛ розглядалася порушення статті 8 в контексті незаконної обробки персональних даних щодо переміщення і місцезнаходження особи.

У справі Шимоволос проти Російської Федерації, російські правоохоронні органи відстежувати інформацію про переміщення заявника, оскільки він був занесений до екстремістської бази – «Сторожовий контроль». Під час однієї з подорожей, заявника неодноразово перевіряли, обшукували та затримували через підозру, що він готується до участі в протестних акціях спрямованих на зрив саміту Росія-Євросоюз [137]. Позиція ЄСПЛ у цій справі полягала у тому, що: «Важливо мати чіткі, докладні правила про застосування секретних заходів спостереження, тим більше, що доступні технології постійно розвиваються … надати громадянам об’єктивну інформацію про умови та обставини, за яких органи влади мають право вдаватися до будь-яких заходів таємного спостереження та збору персональних даних» [137].

Варто зауважити, що дана справа стосується чітко відмежованої сфери обробки персональних даних – обробка персональних даних правоохоронними органами. Така обробка в контексті GDPR має певні специфічні положення, які передбачені як у GDPR, наприклад, параграф 88, який передбачає врахування законних інтересів правоохоронних органів у процедурах повідомлення при витоку даних, так і в національному законодавстві держав-членів ЄС.

Останнім кейсом цього підрозділу буде справа K.U. проти Фінляндії. Ця справа чітко пов'язана з сучасними методами обробки персональних даних, зокрема, з використанням сучасних інформаційних технологій.

За обставинами справи, персональну інформацію заявника було розміщено на сторінці одного із сайтів знайомств, разом з висловами та пропозиціями, що принижують честь та гідність заявника. В той же час, коли батьки заявника (оскільки заявник був малолітньою особою) звернулися до компанії, у чиїй власності знаходився вебсайт для отримання інформації щодо того, хто розмістив таку інформації, компанія відмовилася її надавати, обґрунтовуючи це технічною неможливість отримання такої інформації [138].

ЄСПЛ визнав наявність порушення відразу двох статей – 8 і 13 Конвенції, підтверджуючи позицію заявника щодо того, що незважаючи на те, що діяння особи, що створила фейковий акаунт заявника: «каралося відповідно до Кримінального кодексу, але через недбалість Уряду не було забезпечено те, що Закон про захист приватності та безпеку даних у телекомунікації та Закон про примусові заходи відповідали один одному … негарантована можливість стягнення шкоди від третіх осіб свідчила про недостатність захисту її прав» [138].

Таке прогресивне тлумачення в контексті стабільного розвитку інформаційних технологій повністю відповідає тенденціям передбаченим GDPR.

***

Проаналізована практика правозастосування, однозначно свідчить про дієвість всіх, без винятку, положень GDPR. Підтвердженням цьому є те, що у справах, що аналізувалися, зустрічалося застосування не тільки окремих положень GDPR, але і застосування різних, введених Регламентом, концепцій, як от, наприклад, LSA чи екстериторіальна дія норм GDPR.

Попри відносно однакову практику до тлумачення порушень, наглядові органи різних держав по-різному підходять до оцінки серйозності порушення та визначення міри відповідальності. Особливо яскраво це можна побачити на

прикладах Великої Британії та Іспанії, де попри невелику кількість кейсів Велика Британія має порівняні з Іспанією показники за розмірами призначених штрафів.

Важливо також, що наглядові органи різних країн активно розглядають справи про порушення персональних даних державними органами, особливо у сфері обробки чутливих даних, які найчастіше доступні саме державним установам.

Крім того, в практиці правозастосування норм GDPR яскраво проявляється «інформатизація» суспільства, оскільки з описаних мною кейсів лише один стосувався паперових носіїв даних. Водночас так само один кейс стосувався обробки персональних даних, які людина взагалі не здатна розпізнати.

Продовжуючи тему сучасних технологій варто відзначити, що оскільки GDPR був прийнятий не так давно, він звертає увагу на безліч нюансів обробки персональних даних в мережі інтернет та такої, що здійснюється з використанням соціальних медіа. Зокрема, тут виділяється вимоги GDPR щодо простоти та зрозумілості політик обробки персональних даних, які до цього були надзвичайно великі і не давали потрібного рівня обізнаності користувачам.

Водночас мобільність та гнучкість положень GDPR дозволяє йому взаємодіяти, навіть, з досить складними технологіями, як, наприклад – блокчейн. Такі технології можуть не тільки не протиставлятися, а, навпаки, використовуватися з користю у сфері захисту персональних даних та дотримання GDPR. Особливо увагу окремі дослідники, якщо говорити в контексті блокчейну, звертають на можливість використання цієї технології для шифрування і безпечності передачі даних.

В контексті порівняння механізмів захисту персональних даних за GDPR та в рамках Ради Європи варто відзначити, що попри наявність однакових засад, існують певні відмінності, які потрібно брати до уваги при такому порівнянні. Це зокрема те, що GDPR більше спрямований на регулювання щоденного процесу обробки персональних даних, в той час, як нормативно-правові документи Ради Європи носять більш рамковий характер. Відповідно положення GDPR містяться

більшу деталізацію та більше націлені на контролерів та операторів персональних даних для спрямування їх діяльності в окремих аспектах обробки даних.

Саме ці відмінності пояснюють, наприклад, відсутність в нормативно-правових документах Ради Європи норм спрямованих на створення потужних наглядових органів та посилення відповідальності за порушення правил обробки персональних даних.

Водночас виходячи з практики ЄСПЛ, можна відзначити чіткий напрямок на забезпечення прав людини в окремих випадках та компенсацію порушених прав, що не можна однозначно стверджувати у випадку з GDPR.

ВИСНОВКИ

Проведений в рамках цього дослідження, аналізу дозволяє зробити окремі висновки щодо кожного із поставлених на початку дослідження завдань.

Зокрема, в контексті аналізу теоретичних засад варто відзначити, що з проаналізованого можна стверджувати про загальність принципів обробки персональних, які передбачено в GDPR. Як і в багатьох інших сферах, вони є підгрунтям для формування всіх інших правових норм Регламенту. В контексті GDPR, вони формулюються з врахуванням гнучкості та мобільності сфери захисту персональних даних і тому дозволяють наглядовим органам різних держав застосовуватися їх як джерело для розвитку і тлумачення всіх інших положень GDPR.

З норм, які регулюють діяльність наглядових органів в національних правових системах, випливає чітка тенденція до створення потужних і незалежних наглядових органів у сфері захисту персональних даних. Таке прагнення варто розглядати через призму усвідомлення важливості наявності якісного правозастосування положень GDPR цими наглядовими органами на практиці. Особливо, варто звернути увагу на вимоги щодо незалежності наглядових органів. Найбільшого прогресу щодо цього досягла Італія, оскільки формування наглядового органу цієї країни абсолютно не залежить від уряду країни.

Екстериторіальна дія GDPR активно проявила себе на практиці і не залишилася декларативною нормою, оскільки з аналізу практичних кейсів, можна переконатися, що порушення розглядаються щодо усіх, без винятку, контролерів та операторів персональних даних.

Водночас важливою на практиці є дискреція наглядових органів в підходах щодо визначення розмірів штрафів. Хоча, GDPR передбачає досить великі суми штрафів, на практиці, наглядові органи, часто використовуючи обставини, які впливають на розмір покарання та відступають від запропонованих штрафів.

В контексті, розвитку питання дискреції, варто зазначити, що держави досить часто користуються можливостями змінювати чи уточнювати положення GDPR в національному законодавстві. Особливо яскраво це вирізняється в контексті застосування GDPR до окремих сфер захисту персональних даних. Так, наприклад, досить часто держави приймають окреме правове регулювання для сфери цифрового маркетингу та національної безпеки.

Крім того, окремі країни поєднують регулювання сфери захисту персональних даних з іншими правовідносинами, як, наприклад, Угорщина, де передбачено регулювання захисту персональних даних та забезпечення права на інформацію.

Водночас різко негативне ставлення у ЄС викликає можливість окремих країн відмовлятися від забезпечення права пов’язаних з обігом персональних даних, як це сталося в Угорщині на початку пандемії коронавірусу.

Повертаючись до тематики розвитку та формування наглядових органів, варто зазначити, що аналізовані мною країні відмовилися від створення великої кількості наглядових органів, що мають повноваження щодо захисту персональних даних. Натомість в цих країнах є яскраво виражена тенденція до створення одного потужного наглядового органу, який може мати кілька офісів, існування яких зумовлено специфікою адміністративного поділу держав.

З правозастосовної точки зору, найбільш активно застосовними є положення щодо принципів обробки даних, які часто застосовують у поєднанні з іншими положеннями GDPR. Варто також відмітити, що наглядові органи досить суворо тлумачать всіх принципи вимагаючи від контролерів дотримання, як можна вищих стандартів захисту персональних даних.

Водночас не можна стверджувати про надміру хаотичне тлумачення окремих положень GDPR. Навіть положення щодо зобов’язань контролерів захищати персональні дані від несанкціонованого доступу, на практиці не викликають занепокоєння щодо їх узгодження з можливостями окремих контролерів.

З огляду на відносно недавнє прийняття та достатню гнучкість, GDPR може активно використовуватися для розв'язання конкретних ситуацій пов'язаних з новітніми технологіями. Особливо, це стосується прагнення до простоти та доступності, які закладені в GDPR, що підтверджується вимогами до політики обробки даних, яка має бути зрозумілою для суб'єктів даних.

Водночас деякі сучасні технології, зокрема блокчейн, можуть якісно вдосконалити механізми обробки персональних даних із забезпеченням їх конфіденційності.

В контексті порівняння GDPR та захисту персональних даних в рамках Ради Європи, варто відмітити більш рамковий підхід, який закладений в нормативно-правових актах Ради Європи, який на відмінну від GDPR не спрямований на регулювання щоденної діяльності контролерів. На противагу, варто сказати, що витоки такого правового регулювання є досить схожими, у чому можна пересвідчитися виходячи з принципів обробки персональних даних як у ЄС, так і в рамках Ради Європи.

Водночас практика ЄСПЛ свідчить про спрямованість нормативно-правових документів Ради Європи на забезпечення прав людини в окремих випадках і на компенсацію за порушення таких прав саме суб'єкту даних. В той час як для GDPR питання виплати компенсації не є першочерговим і не висвітлюється в Регламенті, хоча воно є врегульовано в законодавстві окремих країн ЄС, як от у законодавстві Німеччини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The principles. Information Commissioner's Office. Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
2. Regulation (EU) 2016/679 of the European Parliament and of the council of 26 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Jpurnal of the European Union. Електронний ресурс. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1606584609360&from=EN
3. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Український переклад. Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
4. Шаров Даниїл, GDPR: Сутність, принципи, відповідальність за новими правилами обігу персональних даних у ЄС, 02 квітня 2018 року. Електронний ресурс. URL: https://ukrainepravo.com/scientific-thought/legal_analyst/gdpr-sutnist-pryntsypy-vidpovidalnist-za-novymy-pravylamy-obigu-personalnykh-danykh-u-yes/
5. Principle: Lawfulness, fairness and transparency. Information Commissioner's Office. Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/
6. Strawbridge Geraldine, What Are The 7 Principles Of GDPR? July 01, 2019 Електронний ресурс. URL: https://www.metacompliance.com/blog/what-are-the-7-principles-of-gdpr/

7. Quick Guide to the Principles of Data Protection, An Coimisiun um Choisant Sonrai Data Protection Commission, Електронний ресурс. URL: https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf
8. Bhatia Punit, Understanding 6 key GDPR principles. Електронний ресурс. URL: https://advisera.com/eugdpracademy/knowledgebase/understanding-6-key-gdpr-principles/
9. Principle: Data minimisation Information Commissioner's Office. Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/
10. A practical guide to the General Data Protection Regulation, Gregg Latchams Solicitors. Електронний ресурс URL: https://www.gl.law/wp-content/uploads/A-Practical-Guide-to-the-GDPR-Gregg-Latchams-v1-Sept-2017-1.pdf
11. 7 Principles of the GDPR and what they mean, Amara ingenieria de marketing Електронний ресурс. URL: https://www.amara-marketing.com/travel-blog/7-principles-of-the-gdpr-and-what-they-mean
12. Secutiry, Information Commissioner's Office. Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/
13. What are Data Protection Authorities (DPAs)?, European Commission Електронний ресурс. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en#answer
14. Lydia F de la Torre What is a "Supervisory Authority" (SA) under EU Data Protection Law, March 9, 2016, Електронний ресурс. URL: https://medium.com/golden-data/what-is-a-supervisory-authority-under-eu-data-protection-law-5ea69d5b0ea2

15. Guidelines on the Lead Supervisory Authority (wp244rev.01) European Commision, Justice and Consumers, October 31, 2017. Електронний ресурс. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235
16. Богарада Сергій, Територія застосування GDPR, Електронний ресурс. URL: https://legalitgroup.com/teritoriya-zastosuvannya-gdpr/
17. Кулик А. GDPR та український бізнес. 10 непростих запитань, 6 березня 2019, Електронний ресурс. URL: https://biz.ligazakon.net/news/184577_gdpr-ta-ukranskiy-bznes-10-neprostikh-zapitan
18. Territorial scope of the GDPR – Where does the boundary lie? Ashurst, March 04, 2020, Електронний ресурс. URL: https://www.ashurst.com/en/news-and-insights/legal-updates/territorial-scope-of-the-gdpr---where-does-the-boundary-lie/

Цит. 3 Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1. European Data Protection Board, November 12, 2019 Електронний ресурс. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf
19. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1. European Data Protection Board, November 12, 2019 Електронний ресурс. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf
20. FOO Yun Chee, Exclusive: EU privacy chief expects first round of fines under new law by year-end, October 9, 2018, Електронний ресурс. URL: https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY

21. What responsibilities and liabilities do processors have in their own right? Information Commissioner's Office. Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-processors-in-their-own-right/
22. Богорада Сергій, 3 штрафи за GDPR та висновки для українських компаній. Електронний ресурс, URL: https://legalitgroup.com/3-shtrafi-za-gdpr-ta-visnovki-dlya-ukrayinskih-kompanij/
23. GDPR Enforcement Tracker, CMS, Електронний ресурс. URL: https://www.enforcementtracker.com/
24. Духовна Оксана, Вчимося на помилках: найбильгы штрафи за порушення норм GDPR, Юридична Газета № 10 (716), 29 травня 2020, Електронний ресурс. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vchimosya-na-pomilkah-naybilshi-shtrafi-za-porushennya-norm-gdpr.html
25. The risk of GDPR Non-Compliance, Emazzanti Technologies, Електронний ресурс. URL: https://www.emazzanti.net/wp-content/uploads/2018/05/GDPR-Risk-Article-PDF.pdf
26. Договір про Європейський Союз, Маастрихт, 7 лютого 1992 року, Консолідована версія Договору про Європейський Союз і Договору про функціонування Європейського Собзу с протоколами и деклараціями на 30 березня 2010 року. Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/994_029#Text
27. Четверіков А. О. Договір про функціонування Європейського Союзу (нова редакція). Право Європейського Союзу. Електронний ресурс. URL: https://eulaw.ru/treaties/tfeu/
28. Право Європейського Союзу: Підручн. / За ред. Р.А. Петрова. – К.: Істина, 2019. – 392 с.

29. About EDPB, Who we are, European Data Protection Board, Електронний ресурс. URL: https://edpb.europa.eu/about-edpb/about-edpb_en
30. The European Data Protection Board (EDPB). Електронний ресурс. URL: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_en
31. Regulation (EC) No 45/2001 of the European parliament and of the council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on free movement of such data. Official Journal of the European Communities. Електронний ресурс. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN
32. European Data Protection Supervisor. About, Електронний ресурс. URL: https://edps.europa.eu/about-edps_en
33. 5 biggest GDPR fines so far, Data Privacy Manager, January 28, 2021 Електронний ресурс. URL: https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
34. Data protection: The Data Protection Act, GOV.UK, Електронний ресурс, URL: https://www.gov.uk/data-protection
35. Data Protection Act 2018, UK Public General Acts, 2018 c, 12 Електронний ресурс. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
36. What are PECR? Informational Commissioner's Office Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/
37. About the DPA 2018, Informational Commissioner's Office Електронний ресурс. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/#2
38. ICO: Who we are? Informational Commissioner's Office Електронний ресурс. URL: https://ico.org.uk/about-the-ico/who-we-are/
39. ICO and National Privacy Commission, Philippines, sign Memorandum of Understanding, Informational Commissioner's Office, 13 January 2021 Електронний ресурс. URL: https://ico.org.uk/about-the-ico/news-and-

events/news-and-blogs/2021/01/ico-and-national-privacy-commission-philippines-sign-mou/

40. The New Spanish Data Protection Act under the GDPR: What you need to know, Velocity Global, April 29, 2019 Електронний ресурс. URL: https://velocityglobal.com/blog/the-new-spanish-data-protection-act-under-the-gdpr-what-you-need-to-know/
41. Spain GDPR Implementation overview, OneTrust DataGuidance Електронний ресурс. URL: https://www.dataguidance.com/notes/spain-national-gdpr-implementation-overview

    Цит. 3 Ley Organica 3/2018, de 5 de diciembre, de Proteccion de Datos Personales y garantia de los derechos digitales, Legislacion consolidada, Електронний ресурс, URL: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
42. Organical Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. Legal memo, Ecija, Електронний ресурс. URL: https://ecija.com/en/sala-de-prensa/organic-law-3-2018-of-december-5-protection-of-personal-data-and-guarantee-of-digital-rights/
43. Cazalilla A.L., Martin R.B., Spain: Data Protection Laws and Regulation 2020. July 06, 2020 Електронний ресурс. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/spain
44. Cazalilla A.L., Martin R.B., Spain: Data Protection Laws and Regulation 2020. July 06, 2020 Електронний ресурс. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/spain

    Цит. 3 Agencia Espanola Proteccion datos. Official site, Електронний ресурс. URL: https://www.aepd.es/es
45. New Guide on the use of cookies from the AEPD. Cookiebot, Електронний ресурс. URL: https://www.cookiebot.com/es/guia-cookies-aepd/?gclid=CjwKCAiAr6-ABhAfEiwADO4sfTfNq7ekE7WomVZv1x1iS3nrudykIlj-Fd5GZ5SSBhAitYTFRyj3LxoC5tEQAvD_BwE

46. Fares Alkudmani Spanish AEPD Cookie Guidelines: The Ultimate Guide, December 7, 2020. Електронний ресурсю URL: https://secureprivacy.ai/spanish-aepd-cookie-guidelines/

47. Cooper D., Oberschelp de Meneses A., Spanish Supervisory Authority Issues Statement on Data Protection and Coronavirus. Covington, Inside Privacy March 13, 2020, Електронний ресурс. URL: https://www.insideprivacy.com/covid-19/spanish-supervisory-authority-issues-statement-on-data-protection-and-coronavirus/

48. €27,8 million GDPR fine for Italian Telecom – TIM, Data privacy Manager, February 04, 2020, Електронний ресурс. URL: https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/?hsCtaTracking=6680ce94-947d-4fb2-9f28-7d6aa4b9f485%7C76022d76-9c5e-4c0b-a5c6-b1039731b829

49. Italy – Data Protection Overview OneTrust, DataGuidance, Електронний ресурс. URL: https://www.dataguidance.com/notes/italy-data-protection-overview

50. GDPR Italian Implementing Decree has been published. Ma snada M., Berliri M., Colonna M., Mariuz G. September, Hogan Lovells, 14 2018, Електронний ресурс. URL: https://www.hldataprotection.com/2018/09/articles/international-eu-privacy/gdpr-italian-implementing-decree-has-been-published/

51. Personal Data Protection Code Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Garante per la protezione dei dati personali, Електронний ресурс. URL: https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3

52. CMS expert guide: Data law Navigator https://cms.law/en/int/publication/data-law-navigator/italy

Цит. з Personal Data Protection Code Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Garante per la protezione dei dati personali, Електронний ресурс. URL: https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3

53. Italy – Data Prtotection Overview, OneTrust, DataGuidance, Електронний ресурс. URL: https://www.dataguidance.com/notes/italy-data-protection-overview

Цит. з Decreto Legislativo 10 agosto 2018, n. 101, Електронний ресурс. URL: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=false

54. Garante per la protezione dei dati personali. Official site, Електронний ресурс. URL: https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

55. Data Protection&Privacy 2020 - Italy, Chambers and Partners, Електронний ресурс. URL: https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2020/italy Дата звернення: 23.01.2021

56. Specific data protection law and official guidelines in Hungary, Електронний ресурс. URL: https://www.activemind.legal/law/hu-specific-data-protection/

57. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information. Електронний ресурс. URL: https://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf

58. Hungary - Data Protection Overview, OneTrust DataGuidance, Електронний ресурс. URL: https://www.dataguidance.com/notes/hungary-data-protection-overview
59. GDPR Guide to National Implementation: Hungary, White&Case, November 13, 2019, Електронний ресурс. URL: https://www.whitecase.com/publications/article/gdpr-guide-national-implementation-hungary#q3
60. Makszimov V, Hungarian government suspend EU data protection rights. May, 06, 2020, Електронний ресурс, URL: https://www.euractiv.com/section/digital/news/hungarian-government-suspends-eu-data-protection-rights/
61. Stolton S. EU data watchdog "very worried" by Hungary's GDPR suspension, May, 18, 2020, Електронний ресурс. URL: https://www.euractiv.com/section/data-protection/news/eu-data-watchdog-very-worried-by-hungarys-gdpr-suspension/
62. Stepanova O., Feldman J., The privacy, data protection and cybersecurity law review: Germany, October 21, 2020 Електронний ресурс, URL: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-7/1234231/germany
63. Data protection laws of the world, DLA Piper, Електронний ресурс URL: https://www.dlapiperdataprotection.com/index.html?t=law&c=DE
64. Bertermann N. Germany: Data protection laws and regulations 2020, July 06, 2020, Електронний ресурс, URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany
65. Hilberg J. S., The new German Privacy Act: an overview, Електронний ресурс. URL: https://www2.deloitte.com/dl/en/pages/legal/articles/neues-bundesdatenschutzgesetz.html
66. Hilberg J. S., The new German Privacy Act: an overview, Електронний ресурс. URL: https://www2.deloitte.com/dl/en/pages/legal/articles/neues-bundesdatenschutzgesetz.html

Цит. 3 Federal Data Protection Act, June 30, 2017, Електронний ресурс, URL: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

67. Zrinski T., EU GDPR vs. German Bundesdatenschutzgesetz - Similarities and Differences, Електронний ресурс. URL: https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/
68. Runte C., Sandor R., Data Protection and cybersecurity laws in Germany, Електронний ресурс. URL: https://cms.law/en/int/publication/data-law-navigator/germany
69. Federal Data Protection Act, June 30, 2017, Електронний ресурс, URL: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html
70. Gabel D., Dold A., GDPR Guide to national implementation: Germany, November 13, 2019, Електронний ресурс. URL: https://www.whitecase.com/publications/article/gdpr-guide-national-implementation-germany
71. Tasks and Powers: Federal Commissioner fur Data Protection and Free of Information, Електронний ресурс, URL: https://www.bfdi.bund.de/EN/BfDI/Office_Tasks/Tasks/Tasks-node.html
72. Penalty Notice Case ref: COM0759008, ICO, Електронний ресурс, URL: https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf
73. Penalty Notice, Case ref: COM0783542, ICO, Електронний ресурс, URL: https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf
74. ICO fines British Airways £20m for data breach affecting more than 400,000 customers, October 1 16, 2020, ICO, Електронний ресурс, URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

75. Brennan C., UCD fined €70k by data watchdog after email accounts' log-in details posted online, Irish Examiner, February 08, 2021, Електронний ресурс, URL: https://www.irishexaminer.com/news/arid-40222742.html

76. Inquiry into University College Dublin (In-19-7-4), Decision 17 December 2020, Електронний ресурс, URL: https://www.dataprotection.ie/sites/default/files/uploads/2021-02/Inquiry%20University%20College%20Dublin_0.pdf

77. Інформаційний бюлетен 6 (81), листопад 2019б Комісія за защисв на личните данни, Електронний ресурс, URL: https://www.cpdp.bg/index.php?p=element&aid=1219

78. Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro, Електронний ресурс, URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485754#1

79. Keena Colm, Tusla becomes first organisation fined for GDPR rule breach, May 17, 2020, Електронний ресурс, URL: https://www.irishtimes.com/news/crime-and-law/tusla-becomes-first-organisation-fined-for-gdpr-rule-breach-1.4255692?mode=amp

80. Clancy M., Fitzpatrick N., Data Protection Commission Issues First GDPR Fines and Takes Significant Steps re: 'Big Tech' Investigations, Електронний ресурс, URL: https://www.williamfry.com/newsandinsights/news-article/2020/06/18/data-protection-commission-issues-first-gdpr-fines-and-takes-significant-steps-re-'big-tech'-investigations

81. Netherlands: AP fines KNLTB €525,000 for selling personal data to sponsors, OneTrust DataGuidance, March 03, 2020, Електронний ресурс, URL: https://www.dataguidance.com/news/netherlands-ap-fines-knltb-%E2%82%AC525000-selling-personal-data-sponsors

82. The AP's second GDPR fine hits Dutch tennis association with €525,000 penalty, May 27, 2020, Електронний ресурс, URL:

https://www.osborneclarke.com/insights/aps-second-gdpr-fine-hits-dutch-tennis-association-e525000-penalty/

83. Spain: AEPD fines Real Sporting de Gijón €5,000 for unlawful consent collection, OneTrust DataGuidance, July 27, 2020, Електронний ресурс, URL: https://www.dataguidance.com/news/spain-aepd-fines-real-sporting-de-gij%C3%B3n-%E2%82%AC5000-unlawful
84. Spain: AEPD fines LaLiga €250,000 for GDPR violations, OneTrust DataGuidance, Aug, 2019, Електронний ресурс, URL: https://www.dataguidance.com/opinion/spain-aepd-fines-laliga-%E2%82%AC250000-gdpr-violations
85. Spanish football league La Liga fined around €250,000 for a breach of GDPR, June 19, 2019, Електронний ресурс, URL: https://www.fladgate.com/blog-gdpr/2019/06/19/spanish-football-league-la-liga-fined-around-e250000-for-a-breach-of-gdpr/
86. McCaskill S., La Liga Handed $280,000 GDPR Fine For 'Spying' On Fans Watching Pirated Streams, June 12, 2019, Електронний ресурс, URL: https://www.forbes.com/sites/stevemccaskill/2019/06/12/la-liga-handed-e250000-gdpr-fine-for-spying-on-fans-watching-pirated-streams/?sh=2ee3594575d9
87. Data protection update: first UK fine issued under the new GDPR regime, Електронний ресурс. URL: https://amdsolicitors.com/data-protection-update-first-uk-fine-issued-under-the-new-gdpr-regime/
88. Penalty notice to Doorstep Dispensaree Ltd, Електронний ресурс. URL: https://ico.org.uk/media/action-weve-taken/mpns/2616742/doorstop-mpn-20191217.pdf
89. London pharmacy fined after “careless” storage of patient data, ICO, December 20, 2019, Електронний ресурс. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/london-pharmacy-fined-after-careless-storage-of-patient-data/

90. Data protection update: first UK fine issued under the new GDPR regime, Електронний ресурс. URL: https://amdsolicitors.com/data-protection-update-first-uk-fine-issued-under-the-new-gdpr-regime/
91. Decision 20.08.2019 Ref. no. DI-2019-2221 Swedish Data Protection Authority Електронний ресурс. URL: https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf
92. University failed to sufficiently protect sensitive personal data , EDPB, Електронний ресурс. URL: https://edpb.europa.eu/news/national-news/2020/university-failed-sufficiently-protect-sensitive-personal-data_en
93. A Hospital in Portugal receives a fine of 400.000 EUR, Електронний ресурс. URL: https://www.gdprregister.eu/news/hospital-receives-gdpr-fine/
94. Oberschelp de Meneses A, Van Quathem K., Portuguese Hospital Receives and Contests 400,000 € Fine for GDPR Infringement, Електронний ресурс. URL: https://www.natlawreview.com/article/portuguese-hospital-receives-and-contests-400000-fine-gdpr-infringement
95. New record: the Spanish Data Protection Agency fines CaixaBank 6 million euros for violating GDPR, Aguiar R. A. January 22, 2021, Електронний ресурс. URL: https://www.businessinsider.com/httpswwwbusinessinsiderescaixabank-multada-6-millones-euros-vulnerar-rgpd-790971
96. Spain: AEPD fines CaixaBank €6M for consent and information failures, OneTrust, DataGuidance, January 14 2021, Електронний ресурс. URL: https://www.dataguidance.com/news/spain-aepd-fines-caixabank-%E2%82%AC6m-consent-and-information
97. Decision PS/00416/2019, Електронний ресурс. URL: https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf

98. Marolleau L., The French Data Protection Authority imposes a 250,000 euros fine on Spartoo, August 13, 2020, Електронний ресурс. URL: https://www.soulier-avocats.com/en/the-french-data-protection-authority-imposes-a-250000-euros-fine-on-spartoo/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration
99. AEPD, Decision PS/00092/2020, Електронний ресурс. URL: https://gdprhub.eu/index.php?title=AEPD_-_PS/00092/2020
100. Penalty notice, Case ref: COM0804337, Електронний ресурс. URL: https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf
101. ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure, October 30, 2020, Електронний ресурс. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/
102. Datainspektionen, Decision DI-2019-3844, Електронний ресурс. URL: https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-3844
103. Sweden: Datainspektionen fines Aleris Närsjukvård SEK 12M for inadequate technical security measures, OneTrust, Dataguidance, December 04, 2020, Електронний ресурс. URL: https://www.dataguidance.com/news/sweden-datainspektionen-fines-aleris-n%C3%A4rsjukv%C3%A5rd-sek
104. €9.55 million GDPR fine for 1&1 Telecom in Germany, Data privacy manager, December 11, 2019, Електронний ресурс. URL: https://dataprivacymanager.net/e9-55-million-gdpr-fine-for-11-telecom-in-germany/
105. BfDI imposes Fines on Telecommunications Service Providers, EDPB, Електронний ресурс. URL: https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_en

106. Foltýn T., German chat site faces fine under GDPR after data breach, Електронний ресурс. URL: https://www.welivesecurity.com/2018/11/27/german-chat-site-faces-fine-gdpr/

107. Irwin L., Chat app Knuddels fined €20,000 for GDPR breach, Електронний ресурс. URL: https://www.itgovernance.eu/blog/en/chat-app-knuddels-fined-e20000-for-gdpr-breach

108. Montalbano E., AggregateIQ Faces First GDPR Enforcement Over Data-Privacy Dispute, Електронний ресурс. URL: https://securityledger.com/2018/09/aggregateiq-faces-first-gdpr-enforcement-over-data-privacy-dispute/

109. Privacy-Conscious Computer Systems: GDPR Case Study, Електронний ресурс. URL: http://cs.brown.edu/courses/csci2390/2020/assign/gdpr/tjiansin-ilim5-aggregateiq.pdf

110. Чеботарьов К., Конфлікт все ближче. Цукерберг хоче «зробити боляче» Apple у відповідь на нові правила конфіденційності, Електронний ресурс. URL: https://nv.ua/ukr/techno/it-industry/facebook-proti-apple-cukerberg-hoche-zrobiti-bolyache-superniku-ostanni-novini-50142136.html

111. Беца О. Захист персональних даних для Apple, «смерть реклами» для Facebook. За що сваряться техногіганти, Електронний ресурс. URL: https://ms.detector.media/it-kompanii/post/26723/2021-02-26-zakhyst-personalnykh-danykh-dlya-apple-smert-reklamy-dlya-facebook-za-shcho-svaryatsya-tekhnogiganty/

112. Golden D., CCPA, GDPR And The Case For Targeted Advertising Електронний ресурс. URL: https://www.forbes.com/sites/theyec/2019/07/01/ccpa-gdpr-and-the-case-for-targeted-advertising/?sh=729b840726dd

113. Корня А., Захист персональних даних у процесі використання таргетованої реклами та прямого маркетингу, Електронний ресурс. URL:https://uz.ligazakon.ua/ua/magazine_article/EA012761

114. What is targeted advertising? Електронний ресурс. URL: https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/

115. What is Targeted Advertising: Guide, Електронний ресурс. URL: https://sendpulse.com/support/glossary/targeted-advertising

116. Guidelines 05/2020 on consent under Regulation 2016/679, Електронний ресурс. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

117. Захист персональних даних у контексті продажу та просування в інтернеті: національні та європейські вимоги, Електронний ресурс. URL: https://legalitgroup.com/zahist-personalnih-danih-u-konteksti-prodazhu-ta-prosuvannya-v-interneti-natsionalni-ta-yevropejski-vimogi/

118. BLOCKCHAIN AND GDPR - What Can We Learn from the European Parliament's Recent Study? Електронний ресурс. URL: =

119. Blockchain and the General Data Protection Regulation, Електронний ресурс. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf

120. GDPR in Blockchain Environments, Електронний ресурс. URL: https://techgdpr.com/gdpr-tech/gdpr-in-blockchain-environments/

121. GDPR та блокчейн: поєднати непоєднане, Електронний ресурс. URL: https://legalitgroup.com/gdpr-ta-blokchejn-poyednati-nepoyednane/

122. Blockchain and GDPR How blockchain could address five areas associated with GDPR compliance, Електронний ресурс. URL: https://iapp.org/media/pdf/resource_center/blockchain_and_gdpr.pdf

123. Dighmelashvili E., Nanadze A., Kotliarov Y., Tsyba S., Blockchain technology is here – ie it compliant with GDPR? Електронний ресурс. URL: https://www.asterslaw.com/press_center/publications/blockchain_technology_is_here_is_it_compliant_with_gdpr/

124. Kolain M., Wirth C., Privacy by blockchain design: a blockchain-enabled gdpr-compliant approach for handling personal data https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf

125. Romansky R. P. Social media and personal data protection, Електронний ресурс. URL: https://www.researchgate.net/publication/307570419_SOCIAL_MEDIA_AND_PERSONAL_DATA_PROTECTION

126. Confessore N., Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times, Електронний ресурс. URL: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

127. Тарасюк А., GDPR (Загальний регламент про захист даних) – імітація або compliance? Електронний ресурс. URL: https://legalitgroup.com/gdpr-zagalnij-reglament-pro-zahist-danih-imitatsiya-abo-compliance/

128. Trusell R., Copyright and GDPR for photographers, Електронний ресурс. URL: https://ipo.blog.gov.uk/2019/06/11/copyright-and-gdpr-for-photographers/

129. Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С. 2015. — 216 с, Електронний ресурс. URL: https://rm.coe.int/168044e84e

130. Довідник із застосування статті 8 Європейської конвенції з прав людини. Право на повагу до приватного і сімейного життя, житла і кореспонденції, Електронний ресурс. URL: https://www.echr.coe.int/Documents/Guide_Art_8_UKR.pdf

131. The European Convention on Human Rights: A living instrument (2020), Електронний ресурс. URL: https://edoc.coe.int/fr/convention-europenne-des-droits-de-l-homme/8528-the-european-convention-on-human-rights-a-living-instrument.html#

132. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних. Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015, - 220 с.

133. Власюк В., Куц-Карпенко А., Право на захист персональних даних: декілька прикладів із практики ЄСПЛ, Електронний ресурс. URL: https://www.eurointegration.com.ua/experts/2019/01/28/7092096/

134. CASE OF L.B. v. HUNGARY (Application no. 36345/16) JUDGMENT, Електронний ресурс. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-207132%22]}

135. CASE OF AVILKINA AND OTHERS v. RUSSIA (Application no. 1585/09) JUDGMENT, Електронний ресурс. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-120071%22]}

136. CASE OF S. AND MARPER v. THE UNITED KINGDOM (Applications nos. 30562/04 and 30566/04) JUDGMENT, Електронний ресурс. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-90051%22]}

137. CASE OF SHIMOVOLOS v. RUSSIA (Applications nos. 30194/09) JUDGMENT, Електронний ресурс. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-105217%22]}

138. CASE OF CASE OF K.U. v. FINLAND (Applications nos. 2872/02) JUDGMENT, Електронний ресурс. URL: https://hudoc.echr.coe.int/eng#{%22display%22:[%220%22],%22languageisocode%22:[%22UKR%22],%22appno%22:[%222872/02%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-117605%22]}